











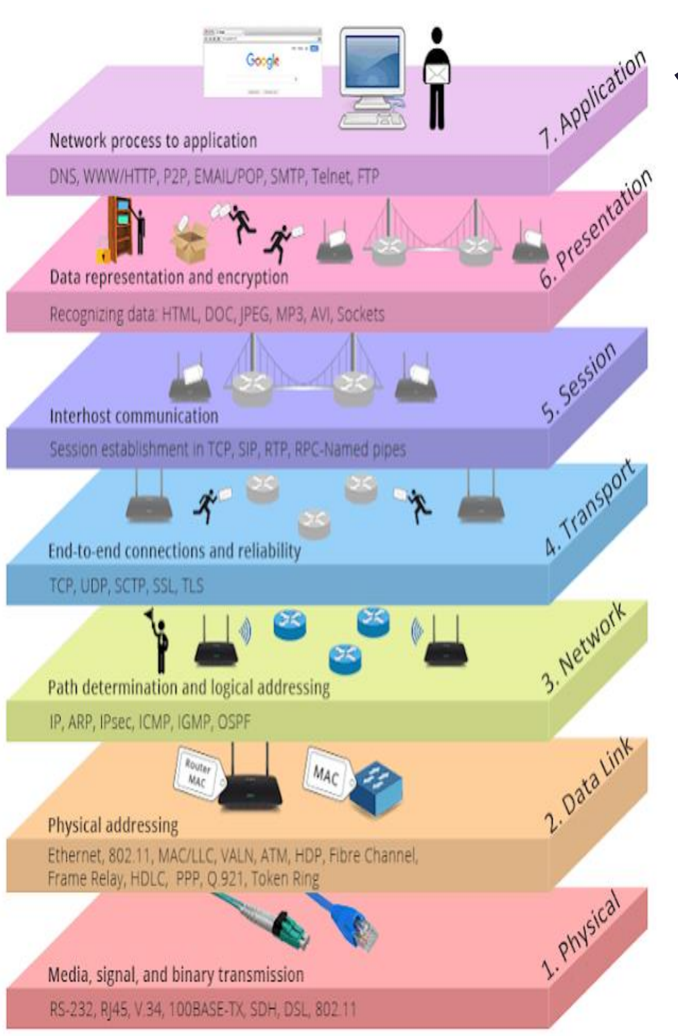


الشبكات مفاهيم تقنية

إعداد

د/ أميرة أحمد

ماجستير العلوم اللغوية الحاسوبية





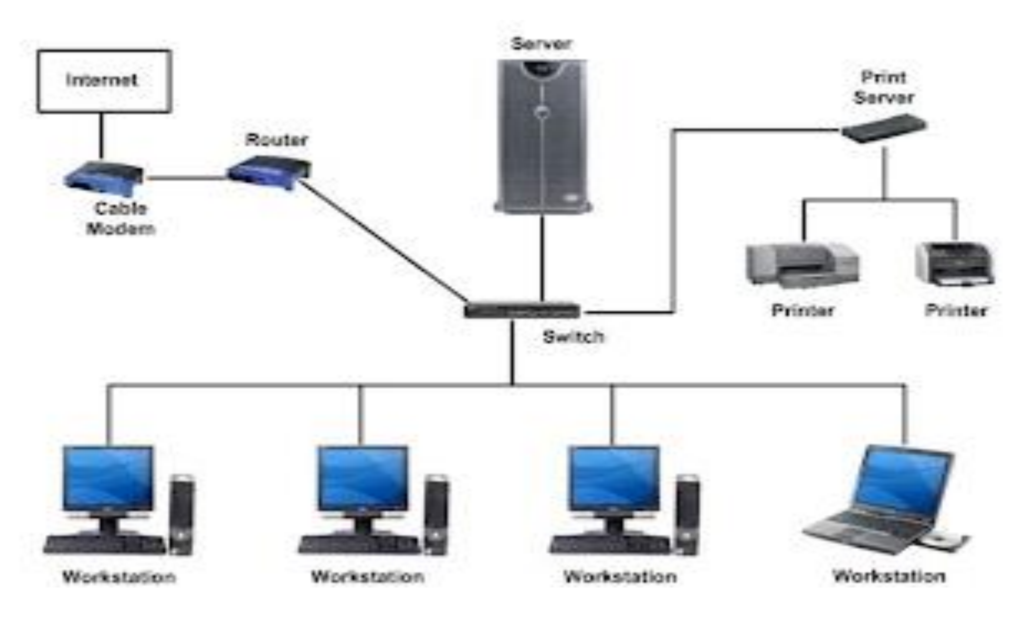


شبكة الحاسوب ومكوناتها:

هي مجموعة من أجهزة الكمبيوتر المرتبطة ببعضها البعض بهدف مُشاركة الموارد، والتطبيقات والخدمات، وإرسال واستقبال البيانات وتبادلها عبر الأجهزة الموجودة ضمن الشبكة.

وتتكون الشبكة من الأجهزة المادية Hardware. والبرمجيات Software.

الأجهزة المادية للشبكة هي مجموعة الأجهزة وبطاقات الشبكة وأجهزة التوصيل كالراوتر والجسر والمحولات، بالإضافة إلى نظام الكابلات الذي يربط بين هذه الأجهزة المختلفة.



(شكل ١ مكونات شبكة الحاسوب المادية)

وعليه كما يتضح من الشكل السابق يمكن حصر مكونات الشبكة المادية في:

١. خادم Server.

٢. محطات عمل Workstation.

٣. كروت الشبكة Network Interface Cards.

٤. كابلات Cabling System.

٥. موارد المشاركةShared Resource .

أما البرمجيات فتتمثل في نظام تشغيل المزود server operating system، وبروتوكولات الاتصال communication protocol، ومسيرات بطاقات واجهة الشبكة network interface card drivers.

وعليه فالمكونات البرمجية في شبكات الحاسوب عبارة عن:

١. نظام تشغيل الشبكات:

عادةً ما يتم تثبيت أنظمة تشغيل الشبكة في الخادم وتسهيل محطات العمل في الشبكة لمشاركة الملفات وقاعدة البيانات والتطبيقات والطابعات وما إلى ذلك.



(شكل ٢ نظم تشغيل الشبكات)

٢. مجموعة البروتوكول:

البروتوكول :هو قاعدة أو مبدأ توجيهي يتبعه كل كمبيوتر لاتصال البيانات، ومجموعة البروتوكول هي مجموعة من البروتوكولات ذات الصلة التي تم وضعها لشبكات الكمبيوتر طبقًا لأحد نماذج الاتصال.

- فئات البروتوكولات

- نموذج "OSI" أي فتح اتصالات النظام.
- نموذج "TCP / IP".

Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP		UDP		
Network Layer	IP	ARP	ICMP	IGMP	
Network Interface Layer	Ethernet	Token Ring	Other Link-Layer Protocols		

(شكل ٣ بروتوكولات الشبكة)

وقد تمّ دراسة الأجزاء المادية المكونة لشبكة الحاسوب في المستوى الأول، لذا ستقتصر دراستنا في هذا المستوى على دراسة برمجيات شبكة الحاسوب؛ وفيما يلي تفصيل ما سبق.

نظام التشغيل الحاسوب:

هو نظام برمجي يعتبر الوسيط بين مستخدم الحاسوب والبرامج والتطبيقات المتنوعة المتواجدة على ذلك الحاسوب، ومن خلاله يمكن للجهاز أن يفهم تعليمات المستخدم، لذلك فإن نظام التشغيل هو ما يقوم بترجمة التعليمات التي يقدمها المستخدم بلغة عالية المستوى إلى لغة الآلة، والتي يمكن للكمبيوتر فهمها.

أنظمة تشغيل الشبكة:

هي أنظمة تشغيل تمتاز بأنها تحتوي على مكونات وبرمجيات تمكّن الحاسب من الاتصال مباشرة بحواسيب أخرى من أجل تنفيذ عمل مشترك، أو لدعم الوصول إلى أدوات وأجهزة أخرى مشتركة مثل الطابعة أو أنظمة تخزين ملفات، أو من أجل الوصول لشبكة أخرى محلية.

ولكل حاسوب داخل الشبكة نظام تشغيل أساسي خاص به، وله ملحقات وخدمات تعمل مع أنظمة التشغيل الأساسية الأخرى، فالشبكة أشبه بحاسوب ضخم مرتبط بآلاف الأجهزة، إضافةً إلى عتادٍ مؤلفٍ من مكونات الشبكة وحواسيبها، بما في ذلك وحدات المعالجة المركزية في جميع الحواسيب والأدوات الأخرى.

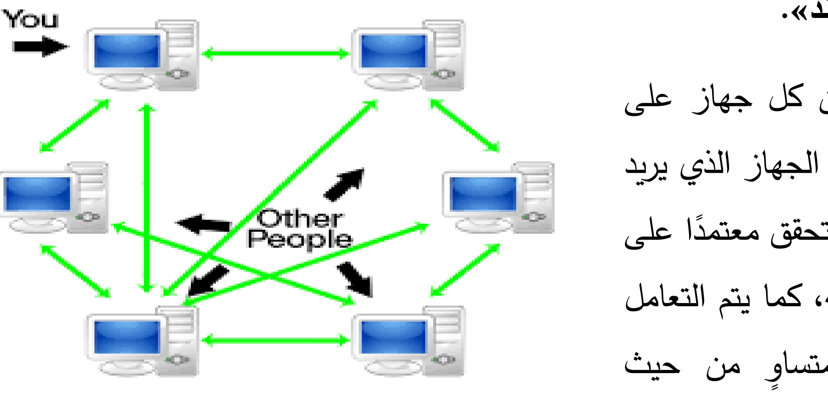
شروط نظام التشغيل الشبكي:

إن مصطلح نظام التشغيل الشبكي يعني نظام تشغيل مبرمج خصيصًا لأجل عمل الشبكات والمحافظة على أمن المعلومات فيها، ويجب أن يتحقق فيه ما يأتي:

١. يتحكم بالشبكة وحركة سير المعلومات مثل حزم البيانات.
٢. يتحكم بصلاحيات وصول المستخدمين إلى موارد الشبكة.
٣. يقدم خدمات إدارة محددة للشبكة بما فيها الأمن الشبكي.

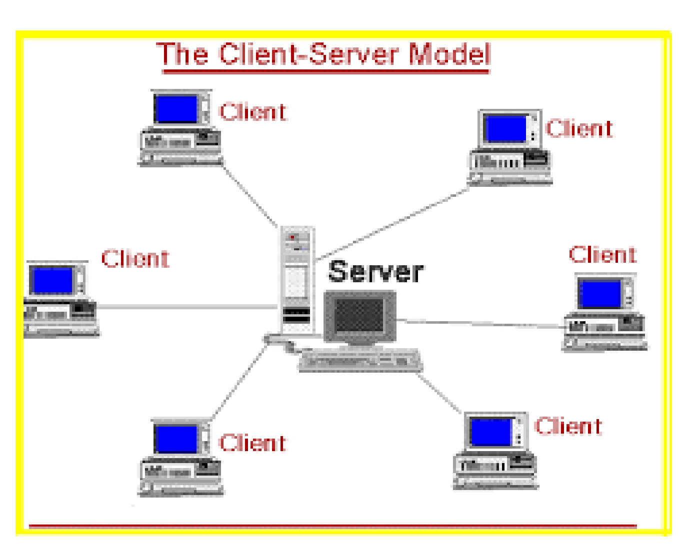
أنماط أنظمة التشغيل الشبكية:

تعمل أنظمة التشغيل الشبكية على نمطين للعمل، ويحدد هذا النمط طبيعة الشبكة ككل، وهما:



- **نمط العمل «الند – للند».**

وفيه يجري التحقق من كل جهاز على حدة على نحوٍ فردي، إذ يطبق الجهاز الذي يريد المُستخدِم الدخول إليه عملية التحقق معتمدًا على معلوماته الخاصة المخزنة لديه، كما يتم التعامل بين جميع الأجهزة بشكل متساوٍ من حيث الوظيفة، ويعمل نمط النظير للنظير عادةً بشكل أفضل للشبكات الصغيرة إلى المتوسطة، كما أنه أرخص كلفة وأسهل في الإعداد.



- **نمط العمل «عميل – خادم».**

وفيه تكون عملية التحقق من هوية المستخدم لدى تسجيل دخوله إلى نظام التشغيل على حاسوبه تحصل مرة واحدة فقط، لأنها تعتمد على الرجوع إلى خادم مركزي يخزن جميع حسابات تعريف المستخدمين، كما يمتلك صلاحية السماح بدخول المستخدم، مما يجعل التغييرات أو الإضافات على باقي أجهزة هذه الشبكة أسهل وأيسر في الاستخدام.

خصائص نظام التشغيل الشبكي:

عادة ما ترتبط خصائص أنظمة تشغيل الشبكة بإدارة المستخدم وصيانة النظام ووظائف إدارة الموارد، وهذا يتضمن:

١. الدعم الأساسي لأنظمة التشغيل مثل دعم البروتوكول والمعالج، واكتشاف الأجهزة الجديدة والمعالجة المتعددة.

٢. إضافة وحذف وإدارة المستخدمين للموارد المتنوعة على الشبكة.

٣. حماية المعلومات والخدمات والأجهزة على الشبكة، ونظام الملفات المشترك وتبادل قاعدة البيانات.

٤. تأمين الدعم الأساسي لمنافذ الأجهزة.

٥. خدمات الخصائص أمن المعلومات كالتحقق من الهوية، وتحديد الصلاحيات، أو تقييد الدخول والتحكم بالوصول.
٦. تأمين إمكانية الوصول للمستخدمين عن بعد، مع أمان الشبكة والمصادقة على المستخدم.
٧. تقديم أدوات لإدارة الشبكة والتحقق من الحسابات ذات واجهات رسومية.

خدمات نظام التشغيل الشبكي:

١. الإذن للمستخدمين بالوصول إلى البيانات في الشبكة، وهذه البيانات عمومًا تُخزن في المخدم.
٢. الإذن للمستخدمين بالوصول إلى بيانات موجودة على شبكات أخرى مثل الإنترنت.
٣. الإذن للمستخدمين بالوصول إلى الأجهزة والأدوات المتصلة بالشبكة، مثل وحدات التخزين والطابعات.
٤. تقديم خدمات التعيين وخدمات الدليل والبحث السريع عن البيانات.
٥. تقديم خدمات النسخ الاحتياطي للبيانات والنسخ المطابق.
٦. تجميع قدرات الأجهزة معًا لكفاءة أفضل في العمل.
٧. تقليل مجال الخطأ والإتاحة العالية لاستغلال الأجهزة.

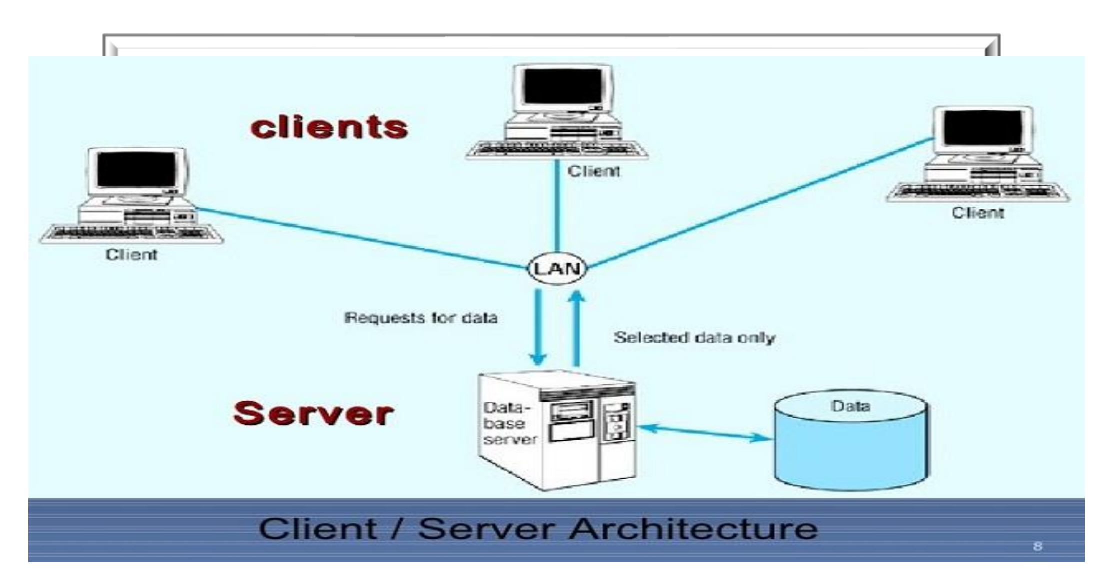
أمثلة على نظام التشغيل الشبكي:

١. **Windows:** وهو الاسم التجاري لمجموعة من نظم تشغيل الخوادم التي أصدرتها مايكروسوفت، ومنه إصدارات (Windows Server 2003, Windows 2000, Windows NT, Windows Server 2008)
٢. **لينكس:** ويسمى أيضًا جينولينكس هو نظام تشغيل حر ومفتوح المصدر، وله توزيعات وأنواع متعددة مثل دبيان وريد هات الشهير، إضافة إلى سوزي وفيدروا.
٣. **Novell NetWare:** هو نظام تشغيل شبكي من صنع شركة نوفل Novell، وهو الأكثر انتشارًا في إدارة الشبكات المحلية الصغيرة والكبيرة وقد قامت شركة نوفل بإعادة تصميمه وإضافة ميزات جديدة إليه، وذلك للعمل بنجاح أكبر في الشبكات الكبيرة وغير المتجانسة كالإنترنت، وهو يدعم عملاء نظام التشغيل دوس، ونظام ويندوز، ونظام ماكنتوش.

وفي الصفحات التالية سنعرض للحديث عن نظام Windows Server، وإصداراته، ونظام لينكس.

١. نظام Windows Server:

أحد منتجات شركة ميكروسوفت مثله مثل أي نسخة ويندوز ولكنها مزودة بإمكانيات مخصصة وبرمجيات خاصة لإدارة وإنشاء الشبكات وإدارتها، وجهاز الكمبيوتر المستخدم كسيرفر أو خادم لابد أن يكون بمواصفات قوية جدًا من حيث العتادHardware ، والبروسيسور CPU والرامات RAM واللوحة الأم Mother Board.



استخداماته:

١. **إدارة شبكة كبيرة محلية تتكون من عدد معين من الحواسيب كشركة مثلا.** فتكون وظيفته إدارة ما يلي:
- كلمات السر ويعطيها لكل جهاز يريد الدخول.

٢. كافة الصلاحيات الباقية لإدارة باقي أجهزة الشبكة ففي حالة تعطله او انغلاقه تتوقف باقي أجهزة الشبكة عن المشاركة والعمل فيما بينهم. وهو ما يعرف في الويندوز سيرفر ب الدليل النشط.Active Directory

تخزين موقع الكترونى. ووظيفته في هذه الحالة:

إدارة وتشغيل المواقع المخزنة على الخادم وذلك بخاصية في الويندوز سيرفر تسمى خدمات معلومات الانترنت أو(IIS) Internet Information Services ، وتسمى هذه الحالة (استضافة) أي أن الموقع تمت استضافته على خادم وأصبح متاحًا للجميع عن طريق الانترنت، كما في شركة جوجل وقسم الداتا سنتر التابع لها وهو المكان الذي يحوي سيرفرات متعددة تستضيف مواقع عدة والداتا سنتر Data Centerمكان مجهز

بكل وسائل التبريد والتهوية الجيدة والطاقة بحيث يكون من غير المحتمل أن يصيب السيرفرات أي خلل في الأداء.

ولعل هذه الاستخدامات هي ما تتطلب عتاداً Hardware بإمكانيات عالية فهو جهاز غير قابل للغلق لأي سببٍ كان لسهولة الولوج إلى الخدمات والبيانات المخزنة عليه.

إصدارات الويندوز سيرفر:

اسم الإصدار	سنة الإنتاج	المميزات
ويندوز سيرفر ٢٠٠٠	**٢٠٠٠**	▪ الأمان ▪ الاستقرار ▪ دعم خاصية DNS
ويندوز سيرفر ٢٠٠٣	**٢٠٠٣**	▪ إدارة عدد أكبر من الشبكات ▪ الأمان والاستقرار ▪ دعم DNS server ▪ توزيع الأتوماتيكي لعناوين الانترنت DHCP server ▪ الدليل النشط Active Directory
ويندوز سيرفر ٢٠٠٨ والنسخة المعدلة windows server R2	**٢٠٠٨**	▪ دعم DNS server ▪ توزيع الأتوماتيكي لعناوين الانترنت DHCP server ▪ الدليل النشط Active Directory ▪ IIS 7
ويندوز سيرفر ٢٠١٢	**٢٠١٢**	▪ دعم DNS server ▪ توزيع الأتوماتيكي لعناوين الانترنت DHCP server ▪ الدليل النشط Active Directory ▪ IIS 8 ▪ الحوسبة السحابية cloud
ويندوز سيرفر ٢٠١٦	**٢٠١٦**	▪ دعم DNS server ▪ توزيع الأتوماتيكي لعناوين الانترنت DHCP server

		▪ الدليل النشط Active Directory ▪ الحوسبة السحابية cloud ▪ Nano server
ويندوز سيرفر ٢٠١٩	٢٠١٨	▪ دعم DNS server ▪ توزيع الأتوماتيكي لعناوين الانترنت DHCP server ▪ الدليل النشط Active Directory ▪ الحوسبة السحابية cloud ▪ IIS10
ويندوز سيرفر ٢٠٢٢	٢٠٢٢	▪ يوفر أمانًا متقدمًا متعدد الطبقات وميزات هجينة فريدة مع Azureومنصة تطبيق مرنة. ▪ تأمين الميزات الأساسية للمساعدة في حماية أجهزة ويندوز سيرفر والبرامج الثابتة ووظائف نظام التشغيل من تهديدات الأمان المتقدمة. ▪ يستفيد الخادم الأساسي الآمن من تقنيات مثل Windows Defender System Guardوالأمان القائم على الظاهرية لتقليل المخاطر من نقاط ضعف البرامج الثابتة والبرامج الضارة المتقدمة. ▪ يوفر الإصدار الجديد أيضًا اتصالاً آمنًا يقدم العديد من الميزات الجديدة مثل اتصالات HTTPS المشفرة الأسرع والأكثر أمانًا وتشفير SMB AES 256 القياسي وغير ذلك الكثير . ▪ يعمل Windows Server 2022 على تحسين إدارة الخادم المختلط من خلال إدارة الجهاز الظاهري المحسّنة بشكل كبير، وعارض الأحداث المحسّن، والعديد من الميزات الجديدة في مركز إدارة Windows. ▪ بالإضافة إلى ذلك، يتضمن هذا الإصدار تحسينات كبيرة على حاويات Windows ، مثل أحجام الصور الأصغر لتنزيل أسرع، وتطبيق نهج الشبكة بشكل أسهل، وأدوات الحاوية لتطبيقات NET.

٢. نظام لينكسLinux:



نظام لينكس هو نظام تشغيل مفتوح المصدر يستخدم في أجهزة الكمبيوتر والخوادم والحواسيب المركزية والأجهزة المحمولة وهو مدعوم على كل منصة كمبيوتر رئيسية تقريبًا مما يجعله أحد أكثر أنظمة التشغيل دعمًا على نطاق واسع.

استخدامات نظام التشغيل Linux

- **إنشاء قواعد البيانات وإدارتها.**

يسمح نظام التشغيل لمديرين قواعد البيانات وضع بعض صلاحيات الوصول لمن يستخدمون قاعدة البيانات. كما يتيح للمستخدمين سهولة الاستخدام وسهولة الوصول للملفات الخاصة بهم.

- **إدارة الخوادم في اصدارات نظام التشغيلLinux**

تعمل معظم الخوادم العملاقة الخاصة بالمواقع الكبيرة تحت مظلة نظام التشغيل.Linux

- **صيانة الحواسيب وأنظمة التشغيل الأخرى**

يعتبر نظام التشغيل Linux من أقوى النظم المستخدمة في صيانة الحاسب الآلي.

- **يمكن لنظام التشغيل أيضاً إصلاح أخطاء أنظمة التشغيل الأخرى.**

من ضمن الخدمات التي يعمل نظام لينكس على تقديمها هي خدمة اصلاح واسترجاع الملفات المحذوفة، وصيانة وإصلاح الأقراص الصلبة.

- **إنشاء المواقع الإلكترونية وإدارتها.**

يوفر نظام التشغيل Linux الكثير من التطبيقات والأدوات والبرامج والتي تساعد مبرمجين المواقع الإلكترونية ومطوريها في بناء المواقع وإدارتها بشكل فعال.

- **بناء الشبكات وإدارتها واصدارات نظام التشغيلLinux**

يعتبر نظام التشغيل Linux من أفضل وأكثر أنظمة التشغيل التي تعتمد عليها الشبكات. وذلك لأن نظام التشغيل Linux يوفر دعم كبير جداً لتشغيل تطبيقات وبرامج إدارة الشبكات.

- **الأمن الالكتروني.**

تعتبر جميع إصدارات نظام التشغيل من أهم النظم في مجال الأمن والحماية الإلكترونية. حيث يعمل نظام التشغيل Linux على صد أي هجمات اختراق إلكتروني، ويحمي الجهاز من الفيروسات المنتشرة على شبكة الإنترنت. كما يحتوي نظام التشغيل لينكس على أداوت خاصة تفيد المتخصصين في مجال الأمن الالكتروني.

إصدارات نظام التشغيل– :Linux

توفر المئات من إصدارات لينكس المختلفة، ولأن لينكس عبارة عن نواة نظام تشغيل و ليس نظام تشغيل متكامل، ظَهر ما يُسمى بالتوزيعات وهي تجميع نواة نظام التشغيل لينكس مع مجموعة من البرامج مفتوحة المصدر و برامج مشروع جنو لينكس ، مما سمح للشركات و المطورين بإصدار و تطوير نسخهم الخاصة من لينكس، وعادةً ما تميز التوزيعات نفسها عن الحزمة من خلال معالجة هدف أو فلسفة أو وظيفة أو سوق مستهدف محدد.

وتتشارك جميع التوزيعات بذات النواة، ولكنها تختلف بالبرامج والتطبيقات الملحقة، وهذا هو سبب وجود توزيعات مختلفة. كل توزيعة من توزيعات لينكس لها مميزاتها الخاصة بها، وقد طورت لتناسب مجموعة معينة من المستخدمين، بعضها يدعم لغة ما وبعضها يعمل كجدار حماية والبعض الآخر يتميز بصغر حجمه، وتحاول بعض من هذه التوزيعات أن تكون مناسبة لطيف واسع من المستخدمين، وذلك لجذب أكبر عدد منهم.

قائمة توزيعات لينكس

- **Arabian Linux**
- **Arabix**
- **CentOS**
- **Damn Small Linux**
- **Debian**
- **Edubuntu**
- **Fedora**
- **Gnoppix**
- **Knoppix**
- **kubuntu**
- **Linspire**
- **Mandriva**
- **MEPIS**
- **PCLinuxOS**
- **Redhat**
- **Slackware**
- **Slax**
- **SuSE**
- **Ubuntu**
- **ututo**
- **Zenwalk Linux**

ولكل توزيعة وظيفة وقد لا تصلح توزيعة مع مستخدم بينما تساعد مستخدم آخر في إنجاز مهامه، فعلى سبيل المثال:

❖ إذا أردت تثبيت نظام لينكس على جهازك وهذه هي المرة الأولى عليك باستخدام إحدى توزيعات أوبنتو Ubuntu.



❖ وللأجهزة القديمة استخدم إحدى توزيعات أوبنتو المتفرعة من أوبنتو Lubuntu او Xubuntu وهذه الأخيرة تستخدم واجهة Xface إحدى واجهات لينكسLunix.



ولاستخدام لينكس بتصميم أقرب ل ويندوز استخدم لينكس منت Linuxmint



النموذج الأول OSI:

الشبكة عبارة عن نظامين أو أكثر من أنظمة الكمبيوتر المرتبطة ببعضها البعض بواسطة شكل من أشكال وسائط النقل التي تمكنهم من مشاركة المعلومات، ولا يهم ما إذا كانت الشبكة تحتوي على اثنين أو آلاف من الأجهزة، فالمفهوم هو نفسه في الأساس .

ولذا توفر الشبكة الخدمات المختلفة لمستخدميها مثل:

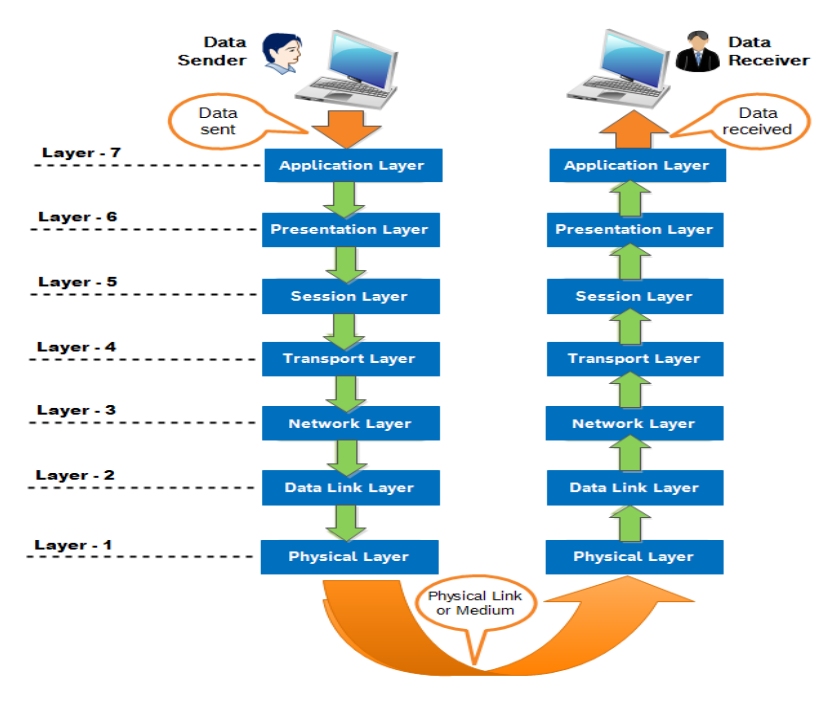
١) الوصول إلى الملفات والمجلدات والطابعات المشتركة.

٢) الوصول إلى تطبيقات البريد الإلكتروني وقواعد البيانات.

٣) الوصول إلى تطبيقات الويب، ونقل الصوت عبر بروتوكول الإنترنت (VoIP)، ومؤتمرات الوسائط المتعددة.

ويمكنك التفكير في أي شبكة من حيث العُقد والروابط، فالعُقد هي أجهزة تتواصل على الشبكة، والروابط هي مسارات الاتصالات بينها.

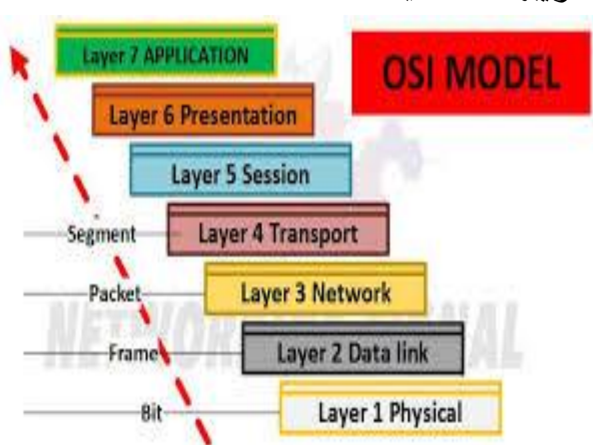
لذا قامت المنظمة الدولية للتوحيد القياسي والمعروفة اختصارًا بـ ISO (أيزو) بتطوير النموذج المرجعي لربط الأنظمة المفتوحة (OSI) في عام ١٩٧٧، وهو اختصار لـOpen System Interconnection هي الطريقة التي بها تستطيع ان تفهم كيفية نقل البيانات عبر الشبكات وقد تم تصميمه للمساعدة في فهم كيفية عمل نظام الشبكة من حيث مكونات الأجهزة والبرامج، وذلك من خلال فصل وظيفة هذه المكونات إلى طبقات منفصلة .



قد يبدو الأمر بسيطاً للمستخدم عند نقل الملفات عبر الشبكة فهو لا يتعدى نقرة زر، إلا أن الأمر ليس كذلك داخل أجهزة الشبكة، فمع زيادة تعقيد أجهزة وبرامج الكمبيوتر، تصبح مشكلة الاتصال الناجح بين أجهزة الشبكة وأنظمتها أكثر صعوبة، لذلك يتيح تقسيم هذه المشكلات الصعبة إلى "مهام فرعية "إمكانية فهمها وحلها بسهولة أكبر، وهنا يأتي دور الـ OSI Modelلنفهم ما الذي يحدث بالضبط.

يتكون OSI Modelمن ٧ طبقات(layers) ، ترتيبها تصاعديًا:

١. الفيزيائية
٢. توصيل البيانات.
٣. الشبكة.
٤. النقل.
٥. الجلسة.
٦. التهيئة.
٧. البرامج.



وتؤدي كل طبقة مجموعة مختلفة من المهام المطلوبة لاتصالات الشبكة، وعلى الرغم من عدم قيام جميع أنظمة الشبكة بتنفيذ الطبقات باستخدام هذا النموذج، إلا أنها تنفذ كل مهمة بطريقة ما، فنموذج OSIليس معيارًا أو مواصفة؛ بل هو بمثابة دليل وظيفي لتصميم بروتوكولات الشبكة والبرامج والأجهزة، ولاستكشاف أخطاء الشبكات وإصلاحها.

معلوم لدينا أن نقل الملفات بين أجهزة الشبكة يتم بين جهازين أحدهما مرسل والآخر مستقبِل؛ لذا علينا الأخذ في الاعتبار أن قراءة هذه الطبقات يتم كالتالي:

- إذا كان الجهاز مُستقْبِل فالاتجاه الخاص بتنفيذ أو نقل البيانات يكون في اتجاه السهم أي من أسفل إلى أعلى؛ بمعنى أن الخطوة تبدأ أولا بـPhysical ثم تنتهي بالـApplication.
- أما إذا كان الجهاز يرسل البيانات فالعكس صحيح. وهو ما يتضح من الشكل السابق.

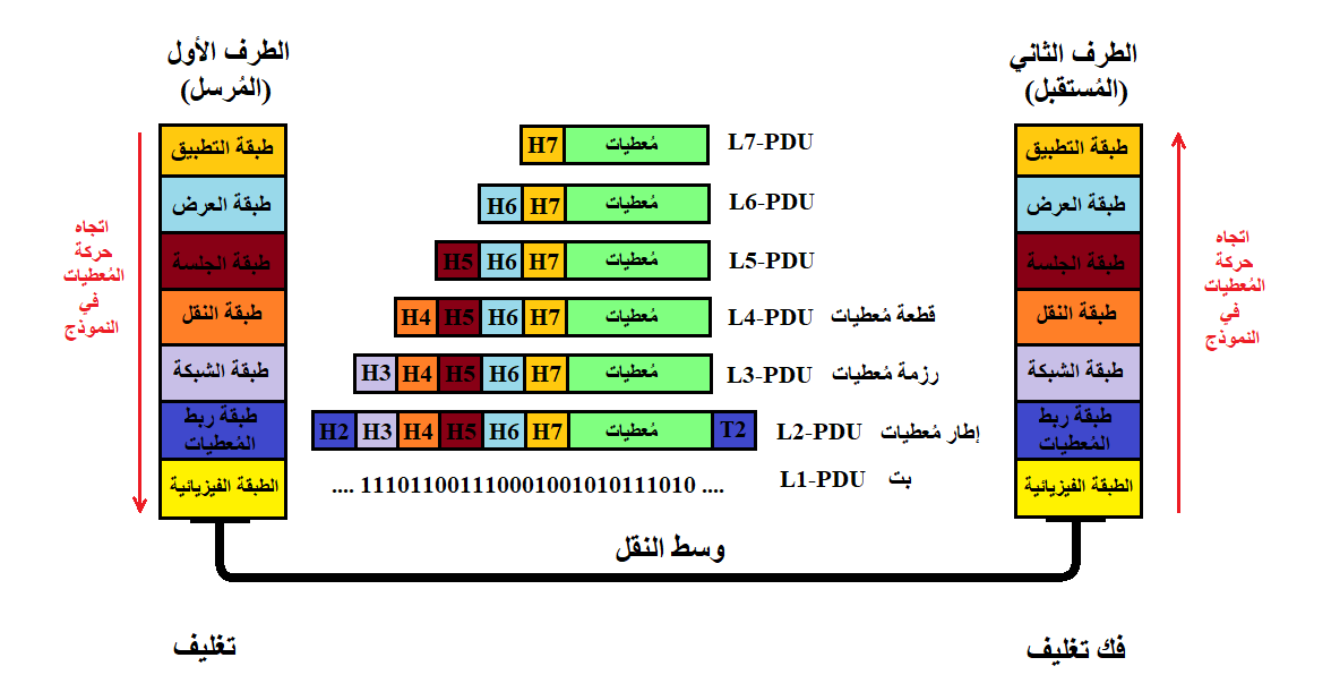
ولتذكر أسماء الطبقات السبعة السابقة فقط تذكر هذه المقولة الشهيرة التي يرددها الكلAll People Seem To Need Data Processing وخذ الحرف الأول من كل كلمة لتعبر لك عن كلLayer

ضع في اعتبارك أن الـ OSI هو مجرد Model أو نموذج يشرح فقط كيفية الاتصال بين جهازين على الشبكة وليس Protocol مستخدم في الاتصال من قبل الأجهزة والبرمجيات!

لقد تم بناء النموذج OSI من سبع طبقات بروتوكول كل طبقة مسئولة عن عمل ما تساعد على تحضير المعلومات من أجل الإرسال وتتفاعل كل طبقة مع جيرانها المباشرين إذ تعرض الطبقة خدمتها إلى الطبقة الموجودة فوقها وتطلب الخدمة من الطبقة التي تحتها.

ولتصور طريقة عمل هذه الطبقات يجب فهم كيف تتم عملية الاتصال بين جهازين على الشبكة؟

تتم عملية الاتصال عند إدخال البيانات المطلوب إرسالها بواسطة التطبيقات، وتنتقل هذه البيانات؛ ويتم ترجمتها بالمرور على كل الطبقات في الجهاز المرسل ابتداءً بطبقة التطبيقات Application، وانتهاءً بالطبقة الفيزيائيةPhysical، حيث تكون البيانات قد تحولت إلى بتات Bits جاهزة للنقل عبر الأسلاك بعد أن تضيف كل طبقة معلومات خاصة إلى البيانات التي يرغب في إرسالها وتسمى هذه العملية التغليف Encapsulation، وعند وصولها إلى الجهاز المستقبل تمر البيانات بطبقات OSI بشكل معكوس ابتداءً بالطبقة الفيزيائية Physical، وانتهاءً بطبقة التطبيقاتApplication ، في عملية تسمى فك التغليف DE Encapsulation، وتكون البيانات الناتجة هي ما يراه المستخدم المستقبِل على جهازه كما هو موضح بالشكل التالي:



وفيما يلي نعرض لكل Layer ووظيفتها والبروتوكولات التي تعمل بها:

١. طبقة التطبيقات أو البرامج Application Layer:

هي الطبقة السابعة من طبقات نموذج "OSI" وهي طبقة مسئولة عن تقديم الخدمات للمستخدم سواء عند إرساله Email أو عمل تنزيل Download لأي مقطع مرئي أو مسموع، أو دخوله لأي موقع على الانترنت كمواقع التواصل الاجتماعي مثلًا. وهي أعلىLayer أو جزء في الـModel وهي لا تعني الـ Applications كبرنامج الـWord او الـAccess وخلافه بقدر ما تعني الـApplication المسؤول عن تنفيذ الأمر المتعلق بالشبكة الذي يطلبه برنامج مثل الـWord ، مثلا عندما تقوم بفتح برنامج عبر الشبكة فأنه يستخدم بعض الأدوات التي لا تراها تسمىTools هذه هي الـApplications المقصودة في المعنى، وتتضمن أيضا الطباعة والرسائل ولا تقتصر على ذلك بل تتعداه.

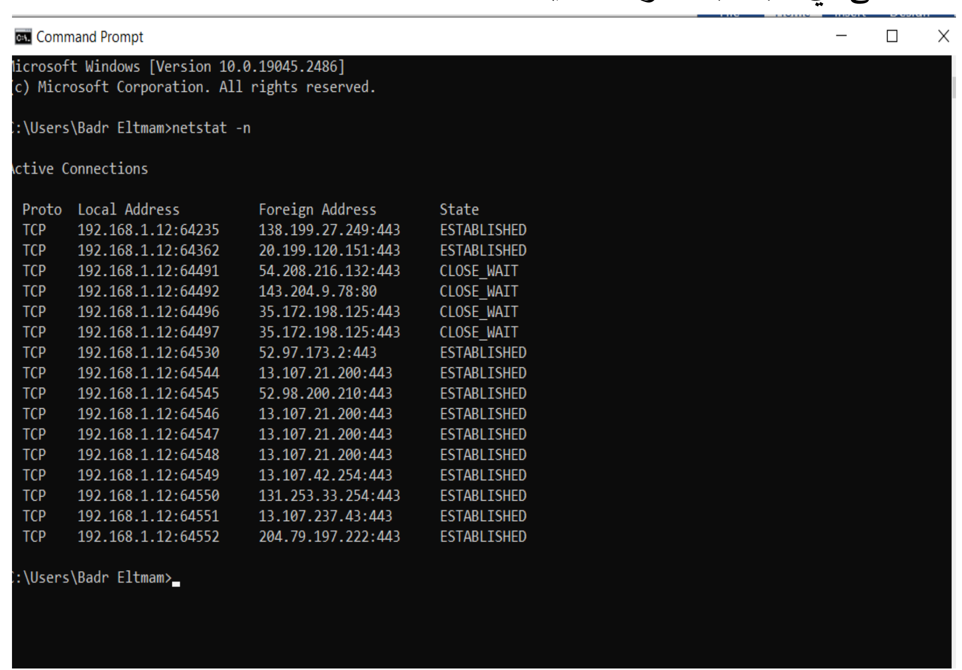
لكل خدمة من خدمات طبقة Application layer رقم منْفَذ Port Number، لطلب الخدمة ولها protocol مسئول عن تنفيذها.

ال **Port Number:** هو رقم ثابت لكل خدمة يتم طلبها من الشبكة، لذا يمكن معرفة كل أنواع الخدمات التي يطلبها كل مستخدم على الشبكة ويمكن المستخدم الوصول إليها.

ال **Protocol:** هو اللغة التي تستخدمها أجهزة الكمبيوتر المتصلة داخل الشبكة مع بعضها، ووظيفة بروتوكول معين داخل طبقة من الطبقات هو المسئول عن تغليف وفك التغليف للبيانات عند مرورها في الطبقة سواء في الإرسال أو عند الاستقبال.

يمكن معرفة الخدمات المستخدمة على أي شبكة بالخطوات التالية:

١. افتح CMD
٢. اكتب الأمر netstat أو –n netstat.
٣. ستظهر كل الخدمات المتاحة كالتالي:

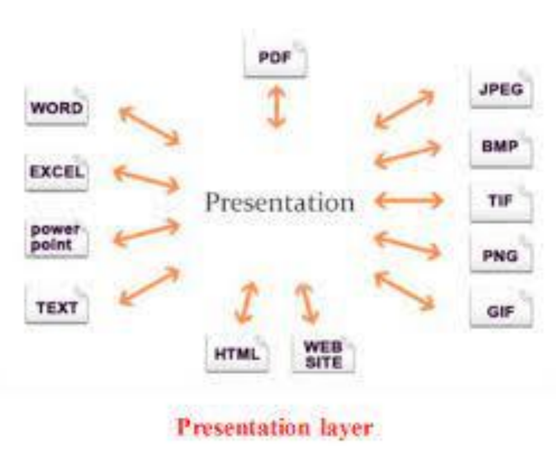


وفيما يلي نعرض لبعض الخدمات وأرقامها والبروتوكولات المستخدمة في طبقة ال Application layer:

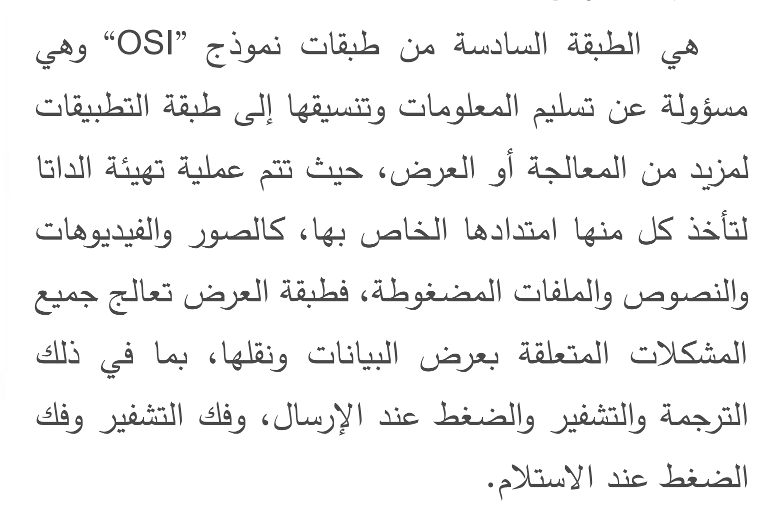
الخدمة	رقم الخدمة	اختصار ل	البروتوكول
المسئول عن التصفح داخل أي موقع، لذا نجده يسبق عنوان أي موقع كالتالي: HTTP://www.google.com	80	Hypertext Transfer Protocol	**HTTP**
أيضًا مسئول عن التصفح إلا أنه أكثر أمانًا، حيث يقوم بتشفير البيانات التي يحصل عليها.	443	Hypertext Transfer Protocol secure	**HTTPS**
لكل موقع اسم يعرفه المستخدم ولكن داخل الشبكة كل اسم يترجم ل IP، وذلك من خلال ال DNS.	53	Domain Name System	**DNS**
هو المسئول عن توزيع ال IP لكل جهاز داخل الشبكة بشكل أوتوماتيكي بدلًا من الطريقة اليدوية.	67 -68 (IP v4) 546- 547 (IP v6)	Dynamic Host Configuration Protocol	**DHCP**
المسئول عن إرسال الرسائل الإلكترونية E-mail	25	Simple Mail transfer protocol	**SMTP**
مسئول عن خدمة رفع وتنزيل الملفات Upload، و Download.	20-21	File Transfer Protocol	**FTP**



٢. طبقة العرض "Presentation Layer":

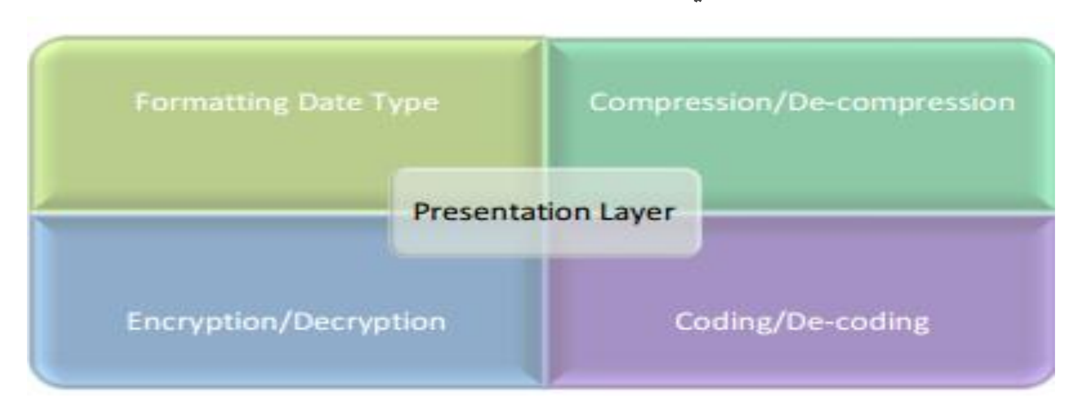


Presentation layer



هي الطبقة السادسة من طبقات نموذج "OSI" وهي مسؤولة عن تسليم المعلومات وتنسيقها إلى طبقة التطبيقات لمزيد من المعالجة أو العرض، حيث تتم عملية تهيئة الداتا لتأخذ كل منها امتدادها الخاص بها، كالصور والفيديوهات والنصوص والملفات المضغوطة، فطبقة العرض تعالج جميع المشكلات المتعلقة بعرض البيانات ونقلها، بما في ذلك الترجمة والتشفير والضغط عند الإرسال، وفك التشفير وفك الضغط عند الاستلام.

لذا فوظيفة هذه الطبقة تنحصر في:



١. **Format**: بمعنى تهيئة الداتا لتأخذ شكلها وامتدادها.

٢. **Compressing and De Compressing**: بمعنى ضغط الملفات وفك الضغط. وذلك لتقليل حجم الداتا لتسريع ال Bandwidth أي عملية نقلها داخل الشبكة على حسب أنواع أجهزة الشبكة.

٣. **Encoding and De Coding**: هي عملية تحويل أي داتا أو كلام إلى Bits بتات (١ & ٠) أي لغة Binary system لغة الآلة، والعكس عند الاستلام على الجهاز المستقبِل أي تحويل البتات إلى داتا أو كلام مرة أخرى.

٤. **Encryption and Decryption**: تشفير البيانات وفك التشفير. وذلك لحماية البيانات أثناء النقل.

ولكل طبقة بروتوكولات تعمل من خلالها وفي طبقة العرض هذه بعض البروتوكولات:

JPEG-MPEG-ASCII-EBCDIC-HTML-AFP-PAD-NDR-RDP- PAD-AVI.

٣. طبقة الجلسة Session layer:

هي الطبقة الخامسة من طبقات نموذج"OSI" ، وهي الطبقة المسئولة عن جلسة العمل من إدارة أي اتصال بين المستخدمين داخل الشبكة؛ مثل فتحه وغلقه، بمعنى آخر هذه الطبقة مسئولة عن جعل المستخدم يستطيع فتح أكثر من موقع في آن واحد فهي تقوم بتنظيم الاتصال بفتح كل موقع في Port منفصل، كما تحدد نوع الاتصال سواء كان إرسال فقط؛ كما في شبكات الرادار والتليفزيون، أو إرسال واستقبال؛ مثل شبكات الهاتف والإنترنت.



Manages connection between client and server

Session Layer هي أول Layer يتعامل معها الـ Users فبدون عمل Open Connection لن يتم إرسال اي Service.

وعليه فهذه الطبقة يتم فيها المهام الآتية:

١. السماح لبرنامجين على كمبيوترين مختلفين إجراء اتصال واستخدام اذه الاتصال وإنهائه بين الجهازين.
٢. التعرف على الأجهزة وأسمائها وإصدار تقارير عن الاتصالات التي تجريها.
٣. الإدارة مثل ترتيب الرسائل المرسلة حسب وقت إرسالها ومدة إرسال كل رسالة.
٤. أخذ عينة من آخر جزء من البيانات تم إرسالها عند توقف الشبكة عن العمل وذلك لكي يتم إرسال البيانات عندما تعود الشبكة الى العمل من النقطة التي توقف عندها الإرسال.

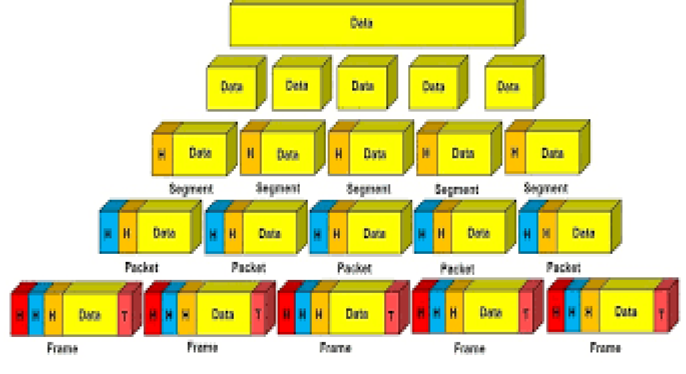
ومن البروتوكولات التي تعمل ضمن هذه الطبقة ما يلي:

- **NFS** Network File System. وهو البروتوكول الافتراضي لنقل الملفات على نظام يونكس ويسمح للمستخدم البعيد بالتحكم بالملفات.
- **SQL** Structured Query Language. بروتوكول يستخدم لعمل اتصال بين المستخدم وسيرفر قاعدة البيانات SQLعلى أنظمة مايكروسوفت.
- **RPC**: بروتوكول يستخدم لعمل اتصال عن بعد وكان يستخدم مع برامج إدارة البريد الالكتروني مثل Outlook.
- **NETBIOS NAME**: وهو بروتوكول يستخدم للتواصل مع الأجهزة قبل ظهور ويندوز ٢٠٠٠ وبعد ظهور ويندوز ٢٠٠٠ تم استخدام بروتوكول TCP/IP بديل عنه.

٤. طبقة النقل Transport Layer:

هي الطبقة الرابعة من طبقات "OSI"، وفيها يتم تقسيم أو تقطيع البيانات Segmentation data إلى حزم أو رزم صغيرة؛ وذلك لأن أجهزة الشبكة (المحولات والموجهات) لديها قدرة استيعاب محدودة لحجم البيانات؛ لذا يجب تقسيم البيانات لقطع عند الإرسال حتى تتمكن أجهزة الشبكة من تسهيل نقل هذه البيانات على شكل قطع من المرسل ومن ثم تجميع القطع وعرضها على المستقبل.

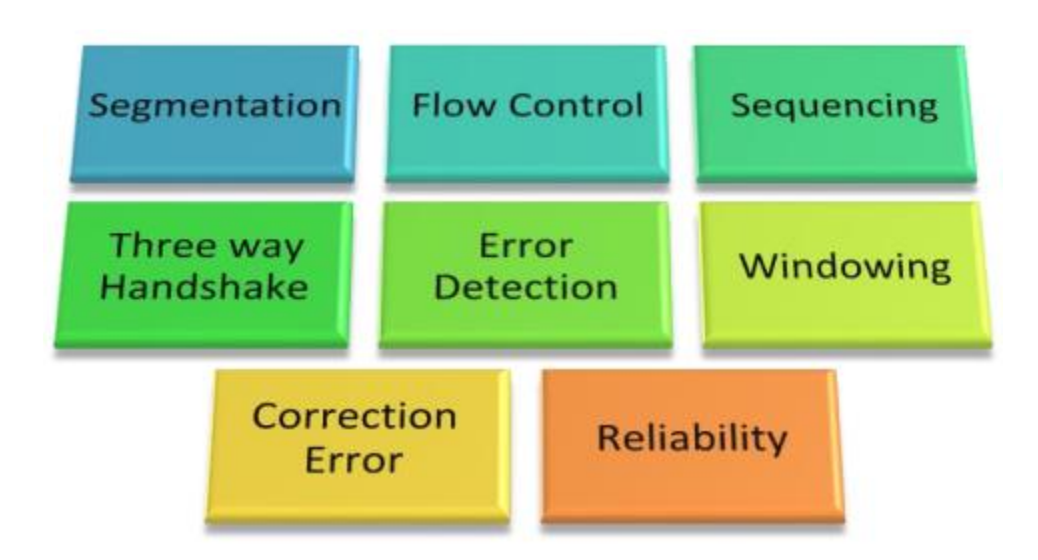
والتقطيع: هو تقسيم الحمولة في بعض طبقات النموذج، إلى قطعتين أو أكثر بحيث تُشكّل كل قطعة حمولة لوحدة بيانات بروتوكول أصغر من وحدة البيانات الأصلية التي تمّ تقطيعُها.



لذا فوظيفة طبقة النقل Transport Layerهي:

١. التحكم في نقل البيانات وتصحيح الأخطاء.
٢. تتم عملية نقل البيانات وذلك بتقطيع الداتا ثم ترقيمها ثم إرسالها والتأكد من وصولها للطرف الآخر.
٣. تحديد طريقة إرسال البيانات هل هي TCP أوUDP .
٤. يتم أيضا وضع البورتات بالتعاون مع طبقة التطبيقات.

ويتم تقسيم الداتا على عدة مراحل هي:



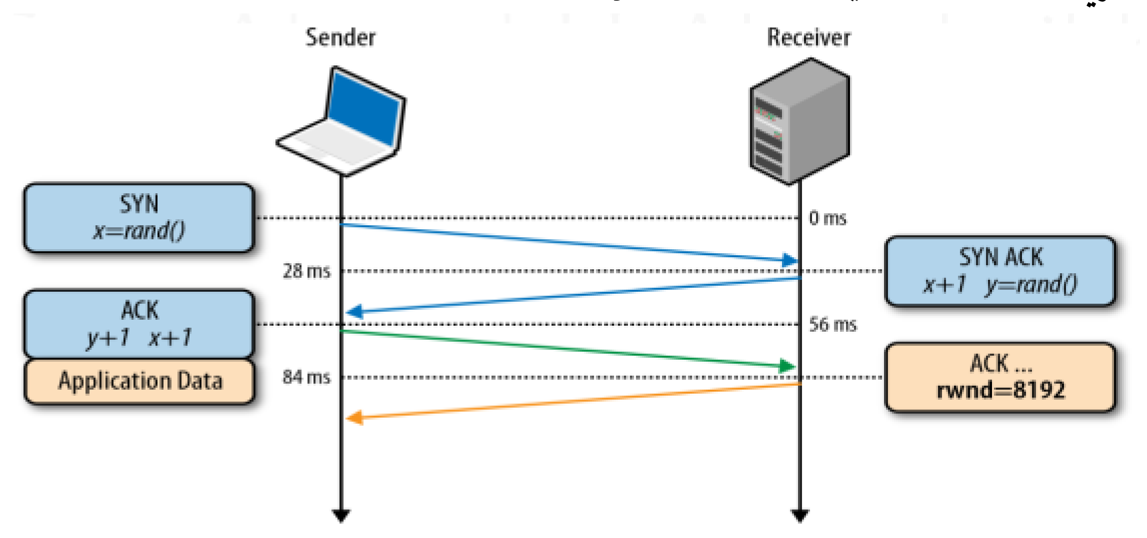
١. التقسيم Segmentation:

يفيد تقسيم البيانات إلى حِزَم صغيرة سهولة الإرسال؛ فإذا حدث خطأ في أحد الحزم كان من السهل عمل تحديد وتصويب Detect and Correct لهذا الخطأ دون الضرر بكامل البيانات، وفي هذه الطبقة بروتوكولان رئيسان هما TCP و UDP، يختلف استخدامهما تبعا لنوع الخدمة المقدمة؛ وسيتم التفريق بينهما لاحقًا.

٢. ترقيم الأجزاء Sequencing:

ويعني بها ترقيم الحزم المقسمة حتى يستطيع الجهاز المُسْتَقْبِل معرفة الكَم الذي استلمه من الحزم المُرسَلة.

٣. طريقة المصافحة الثلاثية Three Way Handshake:

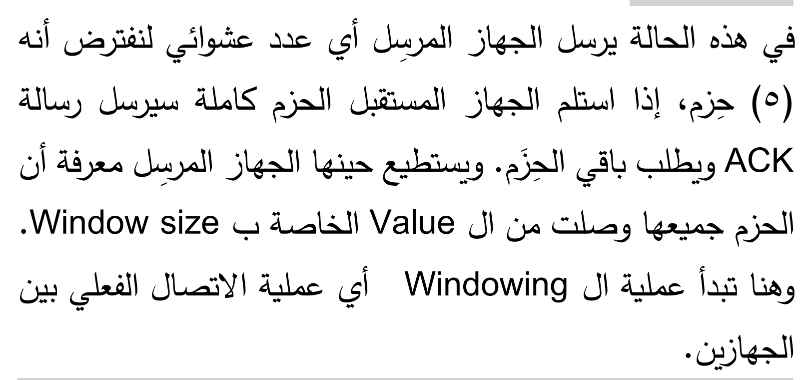


وهي طريقة عمل اختبار Test لل Connection بين الجهازين ال Source وال Destination عن طرق المزامنة وتأكيد التسلم Synchronous and Acknowledge message، حيث يقوم الجهاز المرسل بالإرسال إلى الجهاز المُستقبل للاتفاق على عدد الحِزَم المرسلة وتسمى رسالة المُرسِل ب Synchronous، وإذا كان الجهاز المُستَقبل متاحًا واستلم الحزم يقوم حينها بالرد برسالة تأكيد تسمى Acknowledge message ويقوم بالمطالبة بباقي الحزم المطلوبة في الجلسة.

وفي هذه المرحلة هناك بعض المصطلحات التي يجب معرفتها ولكن يجب وضع سيناريو لشرحها:

بفرض أن لدينا داتا أو حزمة حجمها 150 Byte وتمَّ تقسيمها إلى حِزَم كل منها حجمها 10 Byte، إذن سيصبح لدينا حِزَم عددها ١٥، لنفترض أن الجهاز المرسل لديه قدرة على المعالجة بإرسال 5 Segments في كل مرة للجهاز المستقبل، إذن نحن بصدد حالاتٍ ثلاث:

الحالة الأولى:



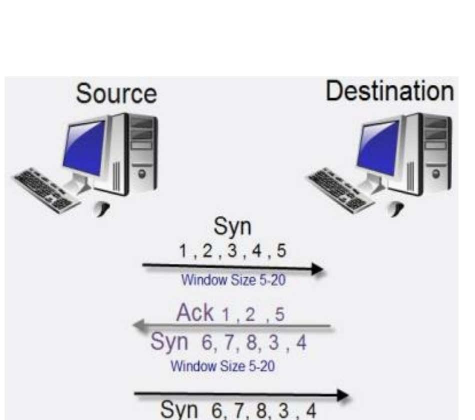
في هذه الحالة يرسل الجهاز المرسِل أي عدد عشوائي لنفترض أنه (٥) حِزم، إذا استلم الجهاز المستقبل الحزم كاملة سيرسل رسالة ACK ويطلب باقي الحِزَم. ويستطيع حينها الجهاز المرسِل معرفة أن الحزم جميعها وصلت من ال Value الخاصة ب Window size.

وهنا تبدأ عملية ال Windowing أي عملية الاتصال الفعلي بين الجهازين.



Window Size: وهو مصطلح يطلق على عدد ال Segments المرسلة في المرة الواحدة من العدد الإجمالي.

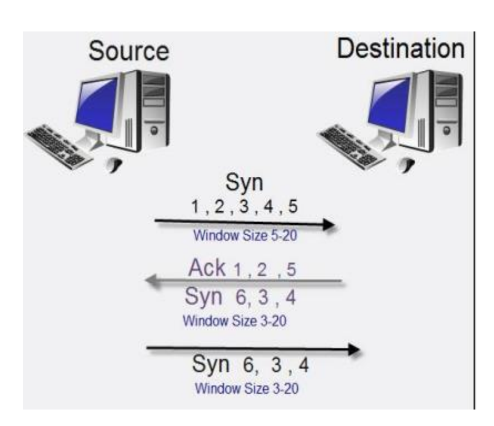
الحالة الثانية:



في هذه الحالة بفرض أن هناك خطأ إرسال في حزمتين ليكن (٣، ٤) لأي سببٍ كان، ولكن حجم ال Window size مازال ثابتًا سيقوم ال الجهاز Destination بإرسال رسالة للجهاز ال Source يُعلمه بما استلمه وما لم يستلمه. والذي اكتشف ذلك الخطأ هو CRC.

Cyclic Redundancy Check (CRC): هي المسئولة عن عمل تحديد وتصحيح Error Detect and Error Correct لأخطاء الإرسال في الحِزَم المرسلة أو المُستلَمة بين الأجهزة.

الحالة الثالثة:



هي حالة حدوث خطأ أيضًا لدى الجهاز المستقبل Destination في الحِزمتين (٣، ٤) أيضًا ولكن الخطأ هذه المرة يسمى Over Flow. وهنا سيطلب الجهاز المستقبِل من الجهاز المُرسِل تعديل ال Window Size على حسب مقدار استيعابه. وهي الحالة الوحيدة التي سيتغير فيها ال Window Size والمسئول عن تصحيح ذلك هي ال CRC. وهذه الحالات الثلاثة هي ما يتم في مرحلة Test For Connection.

Over Flow: هو خطأ يعني أن سرعة نقل البيانات data من الجهاز المُرسِل إلى الجهاز المستقبِل أكبر من معدل استيعاب الجهاز المستقبل للبيانات المُرسلة.

Windowing: عملية بدء الاتصال Connection الفعلية.

ذكرنا سابقًا أن من وظائف هذه الطبقة Transport Layer وضع المنافذ أو ترقيمها Port Number وذلك بالاشتراك مع طبقة التطبيقات Application Layer؛ وذلك حيث تستخدم هذه الطبقة أرقامًا خاصة تكتبها على الحزم قبل إرسالها لتستطيع تمييز بيانات كل برنامج على حدة فتستطيع توصيل هذه البيانات وإرجاع الرد بين جهازي المُرسل والمستقبِل Source and destination.

وعليه فالـ (Ports): هي عبارة عن بوابات أو منافذ اتصال، وتعد جزء من الذاكرة له عنوان معين يتعرف علية الجهاز بأنه منطقة اتصال يتم عبره إرسال واستقبال البيانات ويمكن استخدام عدد كبير من المنافذ للاتصال وعددها يزيد عن ٦٥٠٠٠ منفذ. ويتميز كل منفذ عن الآخر برقمه فمثلا المنفذ رقم ١٠٠١ يمكن إجراء اتصال عن طريقه، وفي نفس اللحظة يتم استخدام المنفذ رقم ٢٠٠١ لإجراء اتصال آخر، يتم الاتصال بين الجهازين عبر الـ ports.

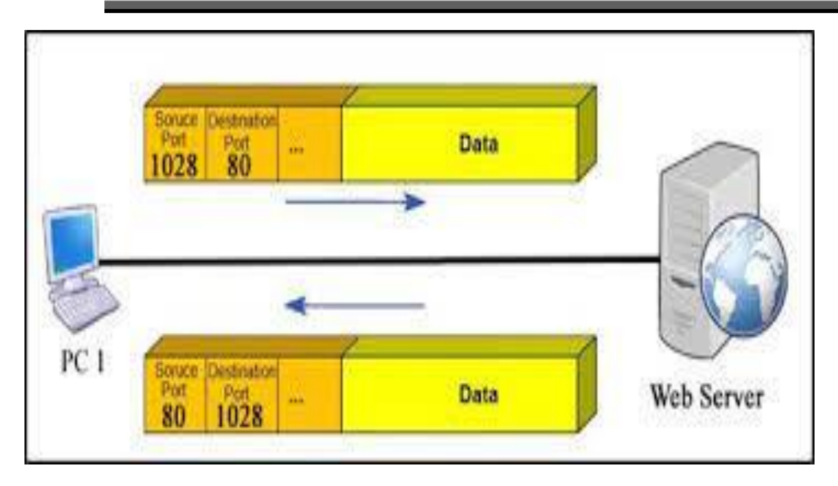
وتنقسم المنافذ الى ثلاثة أقسام هي:

Port Ranges	Category
0 - 1,023	Well-Known Ports
1,024 - 49,151	Registered Ports
49,152 - 65,535	Private/Dynamic Ports

١. **The Well–Known Ports:** هي عبارة عن أرقام ثابتة لصالح تطبيقات معينة تم تحديدها من قبل منظمة INAN و هي تقع في المدى ٠ –١٠٢٣.

٢. **The Registered Ports:** هي التي تقوم الشركات الخاصة بحجزها من أجل تطبيقاتها و هي تقع في المدى ١٠٢٤ – ٤٩١٥١.

٣. **The Dynamic and/or Private Ports:** هي التي لا تكون ثابتة بل متغيرة و هي تقع في المدى ٤٩١٥٢ – ٦٥٥٣٥.



وكل Port هو عبارة عن رقم ١٦ bit يتألف من صفر حتى ٦٥٥٣٥، والـ Ports تنقسم إلى TCP Ports و UDP Portsحسب البرنامج الذي يعمل على هذا الـ Port على سبيل المثال جميع الـ Servers التي تتصل على خدمة Telnet تستخدم الـ Port رقم (٢٣) وهو TCP Port، والـ Web servers تعمل على Portرقم ٨٠ وهو خاص ببرنامجHTTP .

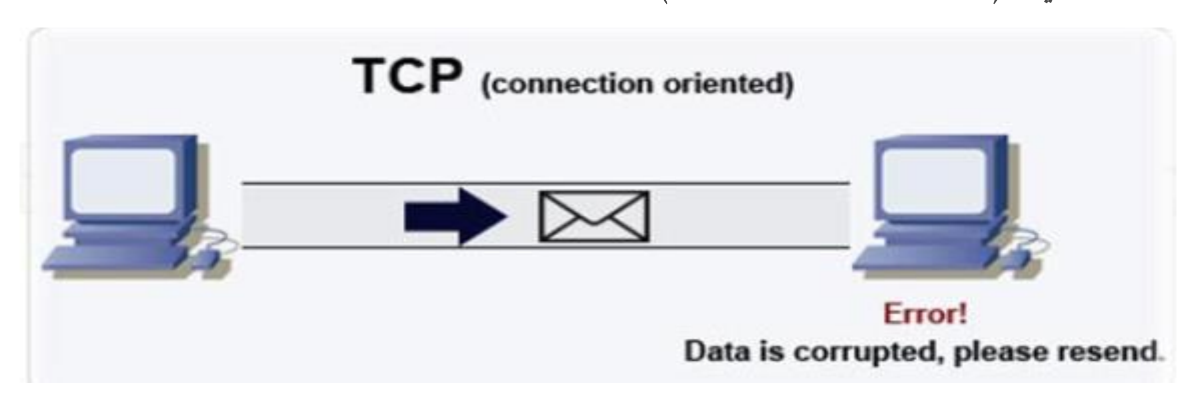
مثال: إذا أرادت طبقة النقل إرسال بيانات باستخدام بروتوكول HTTP إلى جهاز خادم Server لديه بروتوكول HTTP لطلب عرض صفحة معينة سيتم تسجيل Port Number ثابت على هذه البيانات يدل على تطبيق الخادم HTTP وهو الرقم (٨٠) ليكون رقم منفذ الجهاز ال Destination. كما سيتم تسجيل Port Number لجهاز المصدر Source، ويتم اختيار هذا الرقم من نطاق أرقام معين.

بروتوكولات طبقة Transport Layer:

تحتاج طبقة النقل إلى اثنين من البروتوكولات وهما TCP، وUDP، وتحدد أيهما تستخدمه في النقل طبق لنوع البيانات المُرسَلة، كالتالي:

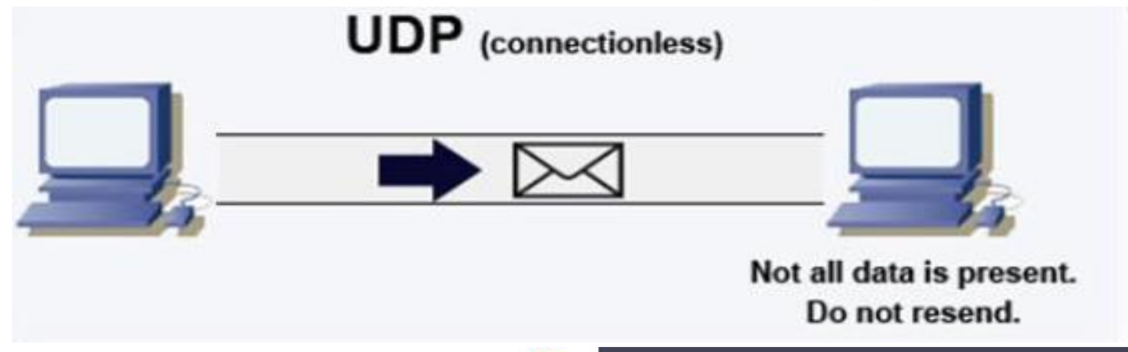
١. **Transmission Communication Protocol (TCP):**

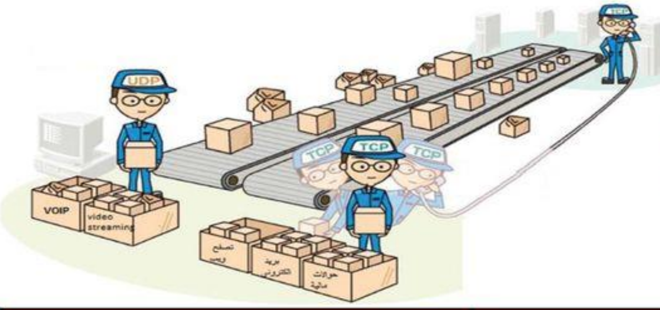
يستخدم في نقل البيانات المهمة؛ فوظيفة هذا البرتوكول تقتضي التأكد من صحة وصول البيانات بشكل كامل، وفي حالة عدم وصول البيانات لأي خطأٍ كان؛ يقوم بإعادة الإرسال مرة أخرى. وهو ما يُطلق عليه طريقة (Connection Oriented).



٢. User Datagram Protocol (UDP):

وهو بروتوكول لا يهتم بتوصيل البيانات بشكل كامل فقط ينقل مرة واحدة؛ ولا يتأكد من سلامة الوصول ولهذه نرى ضعف في إرسال بعض مقاطع الصور أو الصوت. وهو ما يُسمى بطريقة (Connectionless).

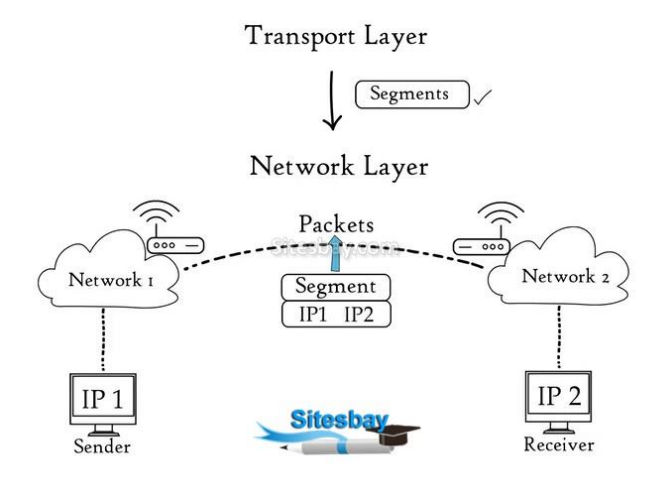




المهام التي تميز بروتوكول الـ TCP عن بروتوكول الـ UDP

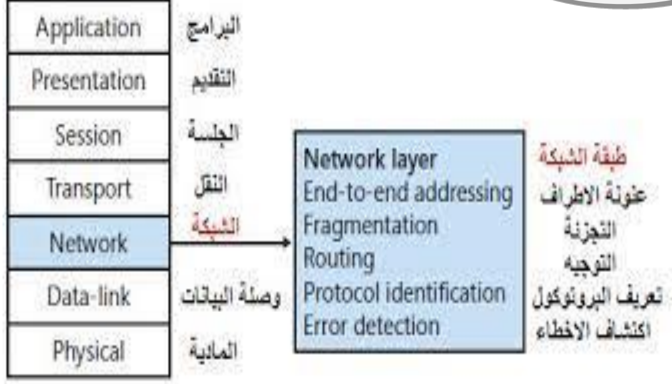
المهام	TCP	UDP
موثوقية البيانات	موثوق	غير موثوق
العبء على الشبكة	يشكل عبء على الشبكة	أقل عبء بكثير مقارنة مع بروتوكول TCP
الخطأ في نقل البيانات	لا تقبل اي نسبة خطأ خلال نقل البيانات	تقبل نسبة معينة من الأخطاء
البيانات المفقودة	يقوم بإعادة ارسال البيانات المفقودة	لا يقوم بإعادة ارسال البيانات المفقودة
سرعة نقل المعلومات	أقل سرعة في التوصيل	سرعة عالية في التوصيل
جودة البيانات	جودة عالية في نقل البيانات	أقل جودة في نقل البيانات
تطبيقات عليها	تصفح الويب، البريد الالكتروني ، التحويلات المالية عبر الشبكة.	الاتصال الهاتفي عبر الشبكة VOIP، بث الفيديو عبر الشبكة video streaming

٥. طبقة الشبكة :Network Layer



هي الطبقة الثالثة من طبقات نموذج "OSI"، بعد تقسيم البيانات في الطبقة السابقة Transport Layer يتم تغليفها فيما يسمى Packet، أي أن كل مجموعة من الحزم ترتبط في غلاف يسمى ال Packet، ويتم وضع ال IP الخاص بجهازي المُرسِل والمستقبِل، ثم يتم إرسال ال Packet. ثم يتم تحديد المسار المستخدم في نقل البيانات وهو ما يسمى بالتوجيه Routing، وذلك باستخدام بروتوكولات النقل والتوجيه داخل الشبكة مثل RIP، BGP، OSPF.

IP: هو عنوان خاص بكل جهاز متصل على الشبكة سواء مُرسِل أو مُستقبِل.



وظائف طبقة الشبكة:

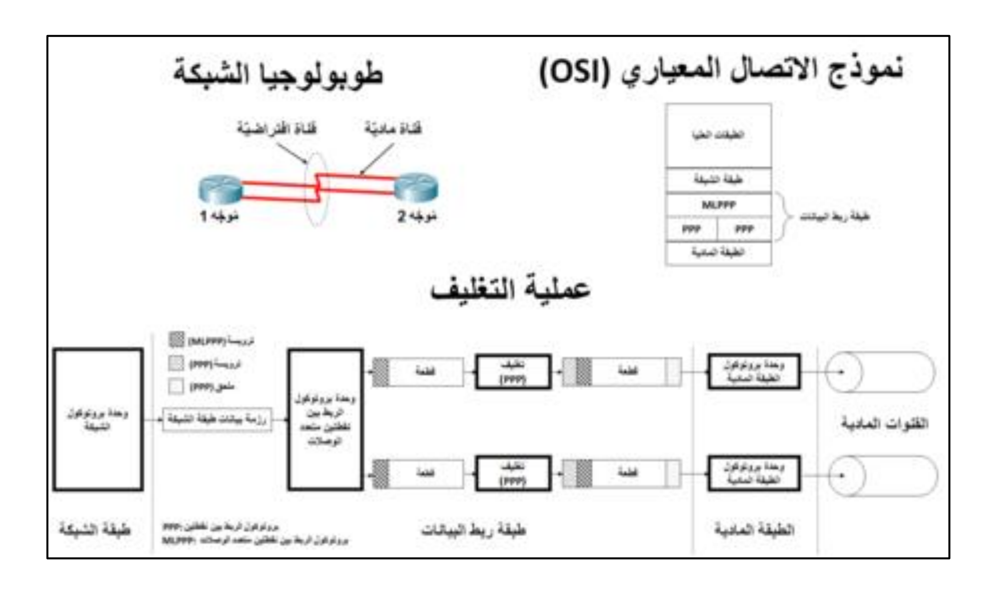
١. تغليف الحِزم وتغليفها في Packet.
٢. عنونة الرسائل وترجمة العناوين المنطقية.
٣. توجيه حِزَم البيانات واختيار أنسب مسار لنقلها بين جهازي المرسل والمستقبل، لتجنب تأخير وصول البيانات أو ضياعها.

بروتوكولات طبقة الشبكة Network Layer:

١. Routing Protocols: بروتوكول التوجيه مسئول عن تحديد أفضل مسار لعملية نقل البيانات بين الأجهزة. أيضا يستطيع ربط شبكات مختلفة معا. ومن بروتوكولات التوجيه RIP, OSPF, EIGRP, BGP.
٢. ARP: تحديد Ip Address، وذلك بمعرفة ال Mac Address.
٣. ICMP: وظيفته عمل test connection وتحدي هل جهاز المستقبل متاح أم لا. كما يستخدم لاختبار الإنترنت بعمل Ping.

٦. طبقة ربط البيانات Data link Layer:

وهي الطبقة الثانية من طبقات "OSI"، وفيها يتم تغليف ال Packet في إطار Frame، وذلك بعد إضافة العنوان المادي MAC Address، للحزم المرسلة.



MAC Address: هو عنوان مادي خاص بكارت الشبكة ، ولا يمكن أن يتكرر على أي جهاز من أجهزة الشبكة، لذلك دائمًا يكون محفور على كارت NIC (Lan card) ، ويتكون من 84 Bits أي 6Byte. ويظهر مكتوبًا بلغة ال Hexa Decimal.

ولمعرفة MAC Address الخاص بجهازك اكتب هذا الأمر في CMD: (ipconfig/all). سيظهر كالتالي:

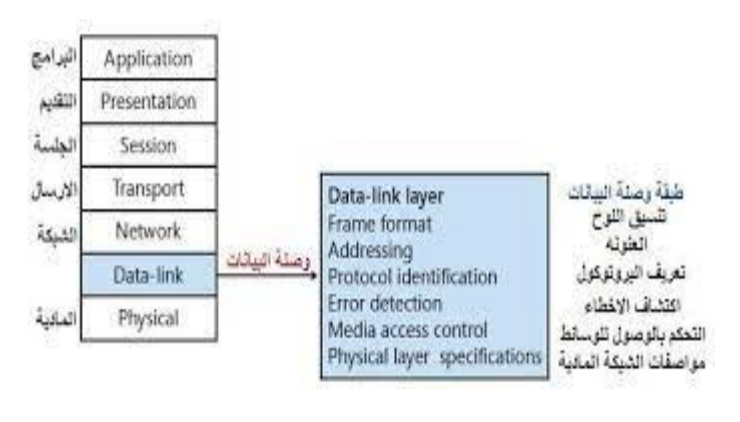
```
Select Command Prompt
   Physical Address. . . . . . . . . : CE-3D-82-B1-33-11
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-N 7260
   Physical Address. . . . . . . . . : CC-3D-82-B1-33-11
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fdd8:2918:5fcf:9d00:ded6:4aa5:4adc:6b68(Preferred)
   Temporary IPv6 Address. . . . . . : fdd8:2918:5fcf:9d00:d0f9:37d4:f654:2c85(Preferred)
   Link-local IPv6 Address . . . . . : fe80::a1bf:a4de:e984:1e3e%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 30 ?????, 2023 02:09:47 ?
   Lease Expires . . . . . . . . . . : 01 ??????, 2023 08:51:39 ?
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 449592706
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-26-60-AB-48-0F-CF-D9-21-51
   DNS Servers . . . . . . . . . . . : fe80::1%20
                                       192.168.1.1
                                       192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

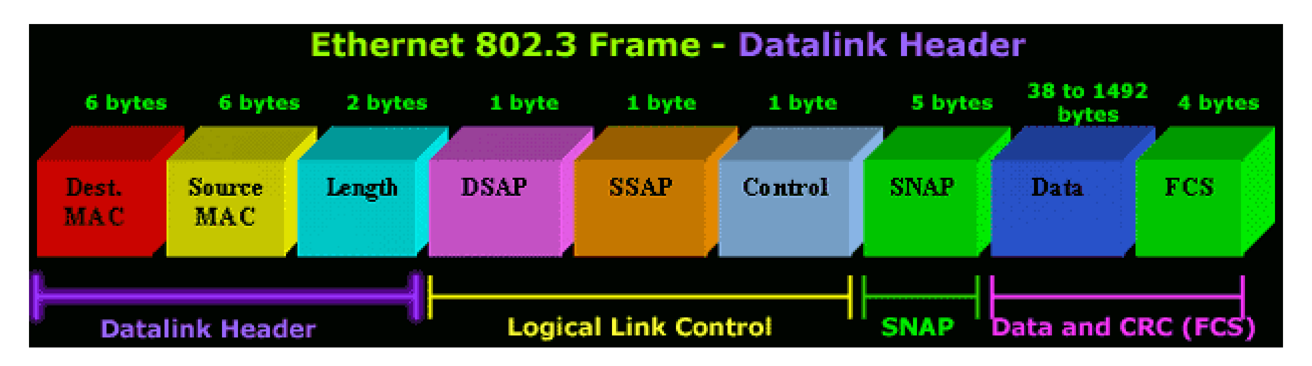
C:\Users\Badr Eltmam>
```

وظيفة طبقة ربط البيانات **Data link Layer**:



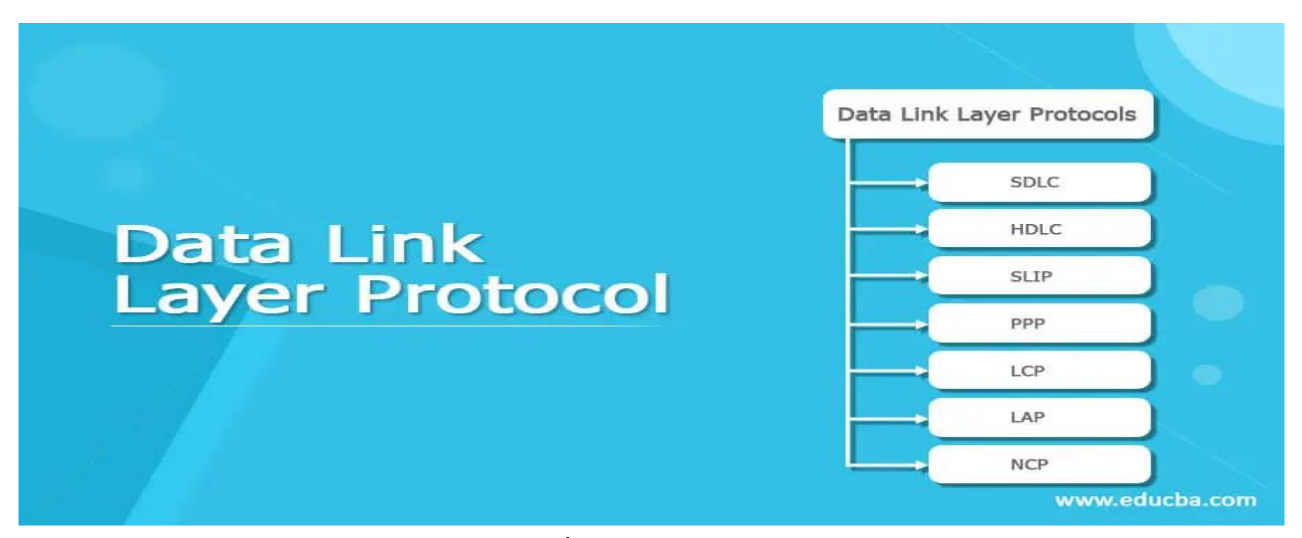
١. تغليف ال Packet وتحويلها إلى Frame. على هيئة رأس وتذييل.
٢. وضع ال MAC Address.
٣. تحديد أفضل وقت لإرسال البيانات وذلك بالتأكد من خلو الكابلات من أي بيانات قبل الإرسال.

ويتم التغليف بوضع ال Packet القادمة من طبقة الشبكة في Frame على شكل رأس وذيل كالتالي:



١. الرأس مكون من **LLC** Logical link control and MAC Address. وفيه يتم تحويل ال Bits إلى Byte ثم تحويلها إلى Frame، ويتحدد نوع وحجم ال **Frame** حسب طريقة التوصيل الخاصة بكابلات الشبكة هل هي **Token ring**، أم **Star**، كما يختلف أيضًا حسب نوع البروتوكول المستخدم. ومن ثم تحديد أفضل وقت للإرسال عن طريق وضع الداتا على الكابل؛ وهناك طريقتان وهما **CSMA/CD** أو **CSMA/CA**، وهما طريقتان لوضع الداتا على الكابل بطريقة لا تتعارض مع وضع جهاز آخر للداتا على الكابل في نفس الوقت.
٢. والذيل **FCR** Frame check Sequence: ومهمته اكتشاف الخطأ فقط دون تصحيحه، الأمر الذي يختلف عن CRC في طبقة النقل Transport Layer.

بروتوكولات طبقة ربط البيانات Data Link Layer:

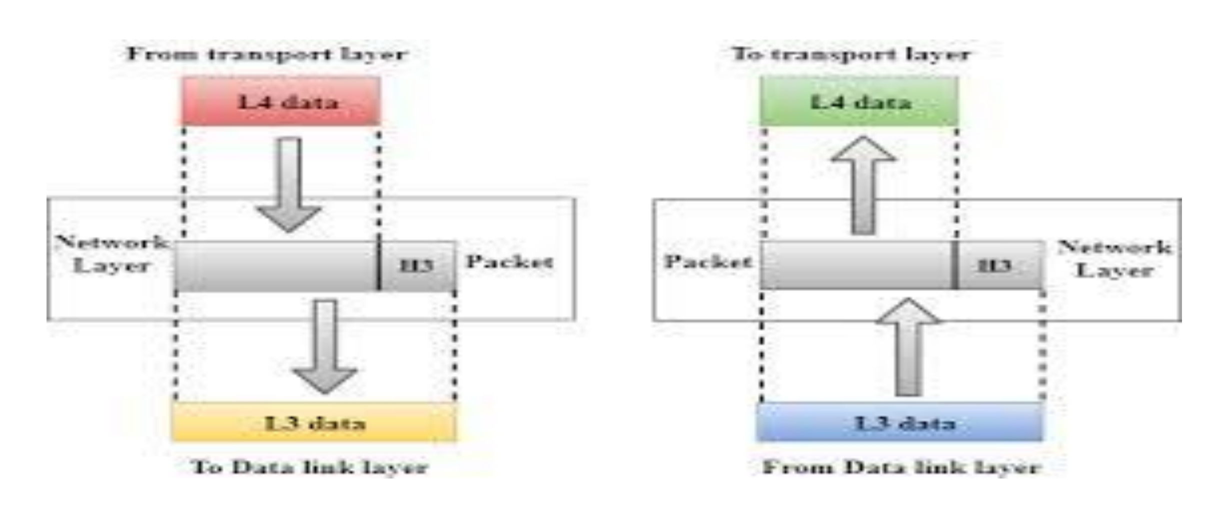


تتعدد البروتوكولات في هذه الطبقة تبعا لاعتبارات كثيرة أهمها نوع الشبكة ومنها:

- LAN protocols: 802.2 (LLC), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless).
- WAN protocols: HDLC, PPP, Frame Relay, ISDN, ATM.

٧. الطبقة الفيزيائية أو الماديةPhysics Layer:

وهي الطبقة الأولى من طبقات "OSI"، وفيها يتم تحويل ال Frameإلى إشارات كهربية عن طريق عمل Coding للرأس Header ككل ويتحول إلى 1/0، ليتم الإرسال عن طريق كارت الشبكة والمودم، ومنه إلى الكابلات ثم إلى الجهاز المُستقبل.



وظائف الطبقة الفيزيائية.

١. تحافظ الطبقة المادية على معدل البيانات (عدد Bits التي يمكن للمرسل إرسالها في الثانية).

٢. تعمل على تزامن Bits.

٣. تساعد في توجيه وسيط الإرسال (اتجاه نقل البيانات).

٤. توفر واجهة بين الأجهزة (مثل أجهزة الحاسوب) ووسيلة النقل.

٥. لديها وحدة بيانات بروتوكول في البت.

٦. يتم استخدام Routers، والإيثرنت، وما إلى ذلك في هذه الطبقة.

٧. تندرج هذه الطبقة ضمن فئة طبقات الأجهزة (نظراً لأن طبقة الأجهزة مسؤولة عن جميع عمليات إنشاء الاتصال المادي ومعالجته أيضاً).

٨. تحويل البيانات إلى موجات راديو عن طريق إضافة المعلومات إلى إشارة عصبية كهربائية أو بصرية.

٩. إعادة توجيه حزم البيانات من منفذ واحد (منفذ المرسل) إلى منفذ الوجهة الرئيسي.

بروتوكولات الطبقة الفيزيائية مشتركة مع بروتوكولات الطبقة السابقة **Data Link Layer**:

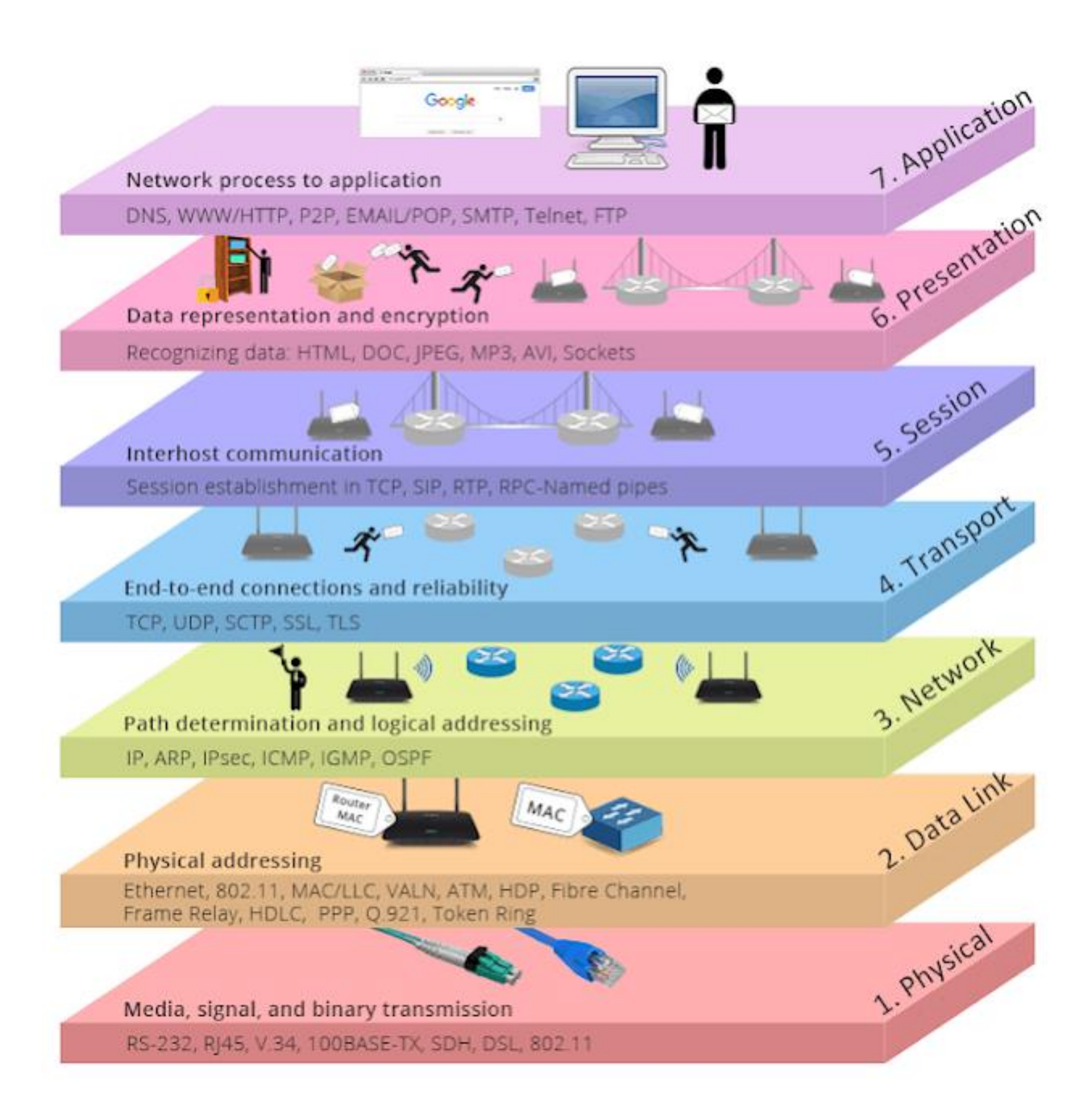
Data Link	LLC Sublayer			
	MAC Sublayer	802.3 Ethernet	802.3 Wi-FI	802.3 Bluetooth
Physical	Physical Layer			

والآن انتهينا من شرح النموذج المعياري لنقل البيانات OSI فهل لاحظت شكل البيانات في الطبقات السبع؟! وماهي الأجهزة Hardware التي تنتقل فيها هذه البيانات؟

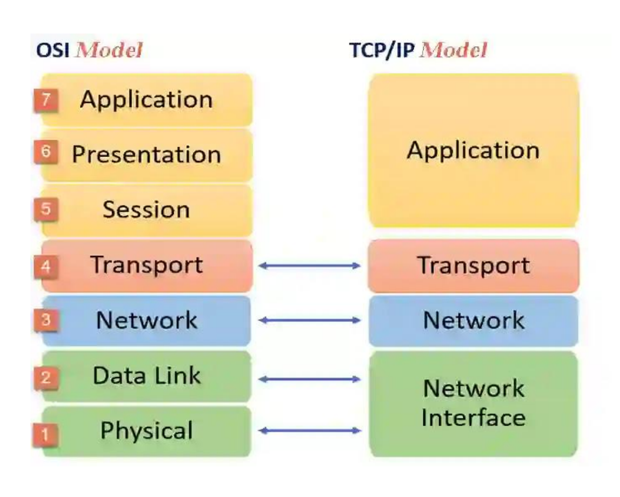
في الجدول التالي سنتعرف على الإجابة:

Layer	Data	Hardware
Application layer	Data	**PC**
Presentation layer	Data	**PC**
Session layer	Data	**PC**
Transport layer	Segment	**Switch Core**
Network layer	Packet	**Router**
Data link layer	Frame	**Switch, HUB**
Physical layer	Bits	**NIC, Cable**

ملخص عمل طبقات ال OSI



النموذج الثانيTCP / IP:



الـ OSI هو مجرد Model أو نموذج نظري ليس له وجود ملموس على أرض الواقع ومهمته فقط شرح كيفية الاتصال بين جهازين على الشبكة– كما ذكرنا سابقًا– فهو ليس Protocol مستخدم في الاتصال من قبل الأجهزة والبرمجيات! أي أنه مجرد نموذج مفاهيمي يوضح مفاهيم ومصطلحات الاتصال داخل الشبكة.

لذا وجب وجود نموذج يساعد أجهزة الشبكة للتفاهم والتعامل فيما بينها بشكل ملموس، ولكي يتم ذلك تتواصل الأجهزة بواسطة مجموعة من البروتوكولات تسمى

"Transmission Control Protocol// Internet Protocol" ويطلق عليها اختصاراTCP/IP .

ومن أجل تطبيق نموذج TCP / IP بشكل مستقل عن نظام التشغيل(windows, Linux, Mac os....) تم تقسيم بروتوكول TCP/IP إلى عدة وحدات بمهمات محددة وبترتيب معين، لنحصل في النهاية على نظام متعدد الطبقات. في هذا النموذج البيانات تمر إلى الشبكة عبر عدة مستويات أو طبقات. وبالتالي، تتم معالجة البيانات (حِزم أو packet) المرسلة على الشبكة في كل طبقة على حدا.

وTCP/IP هو مجموعة من قواعد الاتصال على الشبكة يهدف إلى توفير عنوان IP لكل جهاز على الشبكة من أجل التمكن من توجيه حزم البيانات IP packet. جاء اسم هذا النموذج من البرتوكول TCP والبرتوكول IP لأنهما أول برتوكولان يضافان إلى حزمة برتوكولات TCP/IP.

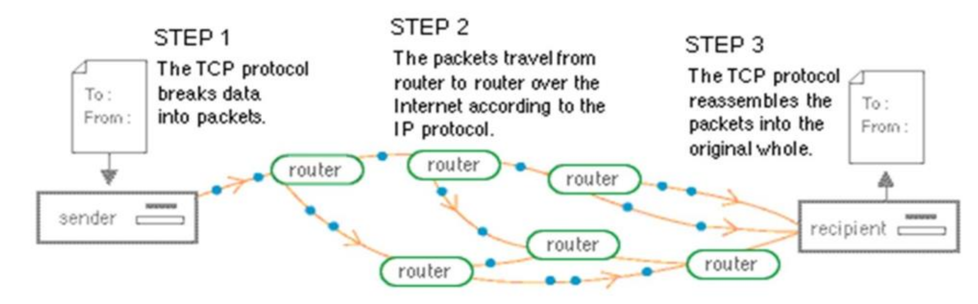


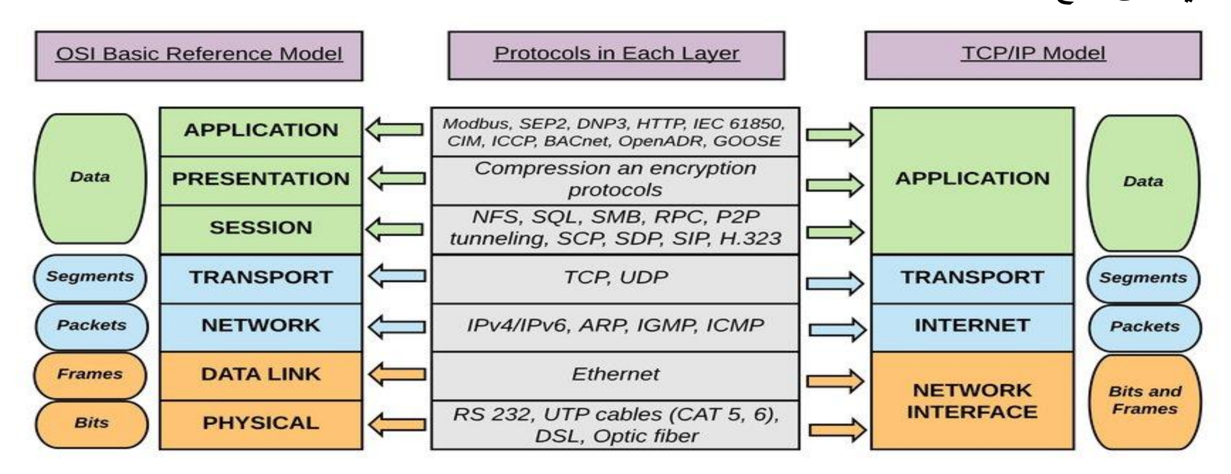
Figure 2. How data travels over the Net.

وقد تمَّ تصميم هذا البرتوكول لتلبية الحاجات التالية:

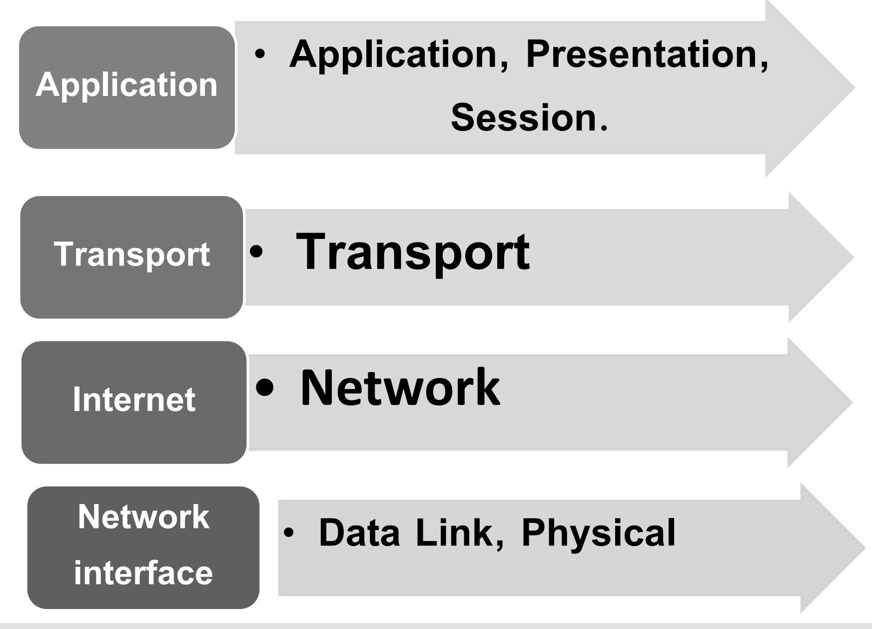
١. تقسيم الرسالة إلى عدة حزم قبل إرسالها في الشبكة.
٢. استخدام عنوان IP خاص بكل جهاز داخل الشبكة.
٣. توجيه الحزم عبر الشبكة (routing).
٤. التحقق من أخطاء الإرسال.

طبقات نموذج TCP/IP:

نموذج TCP/IP مستوحى من نموذج OSI ولكنه يحتوي على أربع طبقات فقط مقارنة مع OSI الذي يحتوي على سبع طبقات.



كما يتضح من الشكل أعلاه؛ فقد تمَّ دمج بعض الطبقات وتغيَّر أسماء البعض الآخر كالتالي:



١. طبقة البرامج أو التطبيقات APPLICATION LAYER :

توجد طبقة البرامج في أعلى مستوى في مجموعة بروتوكول الـTCP/IP ، بحيث تحتوي على كل التطبيقات والبرامج المساعدة والتي تمكن من دخول الشبكة. وتقوم طبقة التطبيقات في نموذج TCP/IP بوظائف الطبقات الثلاث العليا لنموذجOSI ؛ التطبيق، والعرض، وطبقة الجلسة، فهي مسؤولة عن الاتصال من عقدة إلى عقدة وتتحكم في مواصفات واجهة المستخدم. كما تقوم بوظيفة تهيئة وتبادل المعلومات الخاصة بالمستخدم.

بعض البروتوكولات الموجودة في هذه الطبقة هي: HTTP، HTTPS، FTP، TFTP، Telnet، SSH، SMTP، SNMP، NTP DNS، DHCP، NFS، X Window، LPD.

٢. طبقة النقل TRANSPORT LAYER

تشبه هذه الطبقة طبقة النقل Transport Layer الخاصة بنموذج OSI وهي مسؤولة عن إمكانية طلب الاتصال وضمانه بين الأجهزة المتصلة ببعض، أي أن وظيفتها هي الاتصال الشامل والتسليم الخالي من الأخطاء للبيانات. فهي تحمي تطبيقات الطبقة العليا من تعقيدات البيانات .

البروتوكولان الرئيسان في هذه الطبقة هماTCP / UDP، وقد تحدثنا عنهما سابقًا في بروتوكولات النموذج السابق OSI، ولا ضير من التأكيد على طريقة عملهما مرة أخرى .

بروتوكول التحكم في الإرسال :(TCP) من المعروف أنه يوفر اتصالاً موثوقًا وخاليًا من الأخطاء بين الأنظمة الطرفية وينفذ تسلسل البيانات وتجزئتها كما أن لديها ميزة الإقرار وتتحكم في تدفق البيانات من خلال آلية التحكم في التدفق فهو بروتوكول فعال للغاية ولكن به الكثير من النفقات العامة بسبب هذه الميزات وزيادة النفقات العامة تؤدي إلى زيادة التكلفة.

بروتوكول مخطط بيانات المستخدم :(UDP) هو بروتوكول go–to إذا كان تطبيقك لا يتطلب نقلًا موثوقًا لأنه فعال من حيث التكلفة على عكس TCP فهو بروتوكول مهيأ للاتصال فإن UDP غير متصل.

٣. طبقة الإنترنت INTERNET LAYER

تتشابه هذه الطبقة مع وظائف طبقة الشبكة Network Layer في طبقات نموذج OSI، فهي تحدد البروتوكولات المسؤولة عن النقل المنطقي للبيانات عبر الشبكة بأكملها. كما أنها مسؤولة عن تغليف الرزم في وحدات بياناتpackaging ، وتوجيههاRouting ، وتحديد العناوينAddressing .

والبروتوكولات الرئيسة الموجودة في هذه الطبقة هي:

١. **IP:** يعني بروتوكول الإنترنت وهو مسؤول عن تسليم الحزم من المُرسل المصدر إلى المُستقبِل الوجهة من خلال النظر إلى عناوين IP في رؤوس الحزمة ويحتوي IP على نسختين IPv4 وIPv6 .

IPv4 هو الموقع الذي تستخدمه معظم مواقع الويب حاليًا ولكن **IPv6** يتزايد لأن عدد عناوين **IPv4** محدود العدد عند مقارنته بعدد المستخدمين.

ويطلق عليه عنوان الإنترنت IP Address وهو عنوان متفرد ليس له شبيه في النطاق الشبكي ويتميز الـ IP بالتالي:

- **التوجيه Routing**، حيث يقوم بفحص العنوان الموجود على الحِزمة الـ Package ويعطيه تصريح تجول في أرجاء الشبكة، وهذا التصريح له مدة محددة (TIME TO LIVE) فإذا انتهت هذه المدة ذابت تلك الحِزمة ولا تسبب ازدحام داخل الشبكة.
- **تقسيم الحِزَم إلى Packaging وإعادتها.** وفيه يقوم بالتوليف بين بعض أنواع الشبكات المختلفة مثل شبكة الـ Token Ring وEthernet.

٢. **ICMP:** يعني بروتوكول رسائل التحكم في الإنترنت ويتم تغليفه داخل مخططات بيانات IP وهو مسؤول عن تزويد الأجهزة بمعلومات حول مشاكل الشبكة.

٣. **ARP**: وهو بروتوكول مسئول عن تحديد عنوان بروتوكول IP وإيجاد المستقبل الوجهة Destination باستخدام عنوان MAC الموجود في الشبكة للDestination، إذ يقوم الـ IPعند استلام طلب الاتصال بجهازٍ ما يتوجه فورا الى خدمة الـ ARP ويسأله عن مكان هذا العنوان بالشبكة، ثم يقوم البروتوكول ARP بالبحث عن العنوان في ذاكرته فإذا وجده قدم خريطة دقيقة للعنوان، واذا كان الجهاز المستقبل بعيد (في شبكة بعيدة) يقوم الـ ARP بتوجيه الـ IP إلى عنوان الموجه الـROUTER ثم بعد ذلك يقوم هذا الموجه بتسليم الطلب لـ ARP حتى يبحث عن العنوان الفيزيائي MAC Address لرقم الـ IP. ويحتوي ARP على عدة أنواع Reverse ARP :و Proxy ARPو Free ARPو Inverse ARP.

٤. طبقة واجهة الشبكة(NETWORK INTERFACE LAYER)

تتوافق هذه الطبقة مع طبقتي ربط البياناتData Link Layer، والطبقة المادية Physical Layer لنموذجOSI ، فهي طبقة يبحث فيها عن عنونة الأجهزة وتسمح البروتوكولات الموجودة في هذه الطبقة بالنقل المادي للبيانات و ARPهو بروتوكول لطبقة الإنترنت ولكن هناك تعارض حول إعلانه كبروتوكول لطبقة الإنترنت أو طبقة الوصول إلى الشبكة.

وهذه الطبقة مسئولة عن وضع البيانات المراد إرسالها في وسط الشبكة NETWORK MEDIUM واستقبالها منه من الجهاز المستقبل Destination، كما أنها تحتوي على جميع الأجهزة والتوصيلات الخاصة بربط الأجهزة في الشبكة مثل؛ الأسلاك، الموصلات، بطاقات الشبكة.

تحتوي على بروتوكولات تحدد كيفية إرسال البيانات في الشبكة مثل بروتوكول: ATM, Ethernet, Token Ring.

المنفذ Port Addresses في نموذج TCP/ IP

تعلمنا سابقًا أن الجهاز لكي يستطيع فتح أكثر من جلسة عمل Session يجب أن يحتوي على منافذ لكل منها رقم خاص، وهذه الأرقام قد تكون محجوز ومحددة وقد تكون عشوائية، والأمر لا يختلف بين نموذج OSI وبين الـTCP/IP.

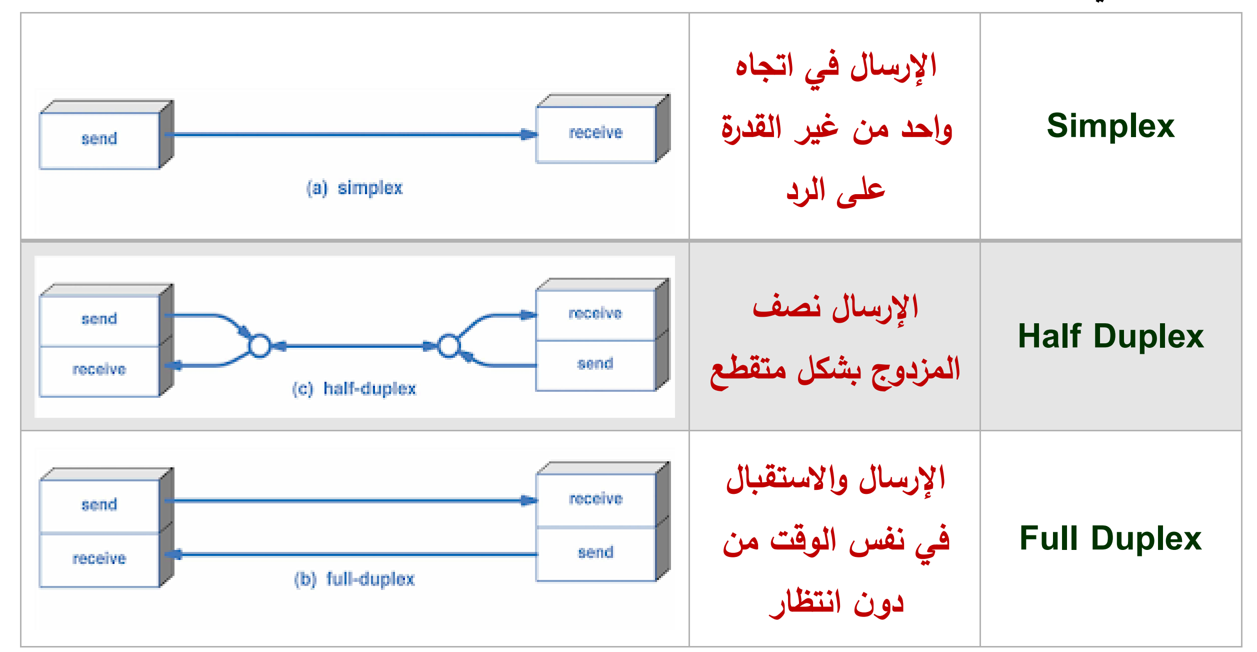
وخلاصة القول هذه أهم نقاط التشابه والاختلاف بين نموذجي OSI، وال TCP/IP:

TCP/IP	OSI
له وجود ملموس يتم التعامل معه	مجرد نموذج مفاهيمي
يشير TCP إلى بروتوكول التحكم في الإرسال	يشير OSI إلى ربط الأنظمة المفتوحة
يحتوي TCP / IP على ٤ طبقات	لديها ٧ طبقات
أكثر موثوقية	أقل موثوقية
ليس لديها حدود صارمة	لديها حدود صارمة
يتبع نهجًا أفقيًا	يتبع نهج عمودي
يستخدم كلاً من طبقة الجلسة والعرض التقديمي في طبقة التطبيق نفسها	يستخدم طبقات جلسة وعرض مختلفة
طورت بروتوكولات TCP / IP ثم النموذج	طور OSI النموذج ثم البروتوكول
لا توفر طبقة النقل في TCP / IP ضمانًا لتسليم الحزم	في نموذج OSI توفر طبقة النقل ضمان تسليم الحزم
توفر طبقة شبكة نموذج TCP / IP خدمات اتصال أقل فقط	يتم توفير اتصال أقل وتوجيه اتصال كلا الخدمتين من خلال طبقة الشبكة في نموذجOSI
لا يمكن استبدال البروتوكولات بسهولة في نموذج TCP / IP	تتم تغطية البروتوكولات بشكل أفضل ويسهل استبدالها بالتغيير في التكنولوجيا

أولًا: طرق إرسال البيانات في الوسط المادي للشبكات

Methods of Sending Data in the Physical Media Networks

توجد ثلاث طرق لعلمية إرسال البيانات في أجهزة الشبكة، أو الوسط المادي الفيزيائي على مختلف أنواع الأجهزة. وهي:



Simplex	الإرسال في اتجاه واحد من غير القدرة على الرد
Half Duplex	الإرسال نصف المزدوج بشكل متقطع
Full Duplex	الإرسال والاستقبال في نفس الوقت من دون انتظار

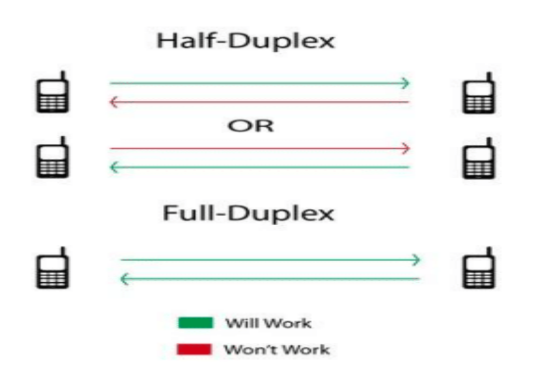
(Simplex)

يوفر نظام الإرسال في اتجاه واحد الإرسال فقط من دون الاستقبال أو الرد على المرسل مثل شبكات الراديو والتلفزيون.

(Half Duplex)

يوفر نظام الإرسال نصف المزدوج عملية اتصال في كلا الجانبين، لكن بالسماح باتجاه واحد في وقت ما غير متزامن، أي أن رد الاتجاه الآخر يتم في وقت آخر، فعندما يبدأ أحد الأطراف باستقبال إشارة ما، فإنه يبقى منتظراً حتى يتوقف المرسل عن عملية الإرسال، قبل الرد. ويعد جهاز اللاسلكي (ووكي توكي) أحد أبرز الأمثلة على هذا النوع، فعملية الاتصال ممكنة بين الطرفين إلَّا أنه في الوقت الذي يتحدث فيه أحدهما ينبغي للآخر الاستماع حتى الانتهاء بتحرير زر الاتصال وبالتالي يمكن للأخير ضغط زر الاتصال لبدء دوره وذلك لأن كلا الطرفين يبثاه عبر تردد واحد.

(Full Duplex)



يسمح نظام إرسال الازدواج الكامل بالتواصل في كلا الاتجاهين وفي نفس الوقت، على العكس من الازدواج النصفي. تمثل خطوط الهاتف المحلية والهاتف النقال أمثلة على هذا النوع من الاتصالات. في جهاز الكمبيوتر يمكن أيضاً القول بأن الإيثرنت تعمل بنفس المبدأ.

ولكي تتم عملية الاتصال بالازدواج الكامل ينبغي أن يكون هناك اختلاف مميز بين الطرفين مثل استعمال ترددين مختلفين لمنع تداخل الإشارات أو باستعمال مداولة ذات تقسيم زمني بمعنى أن يتم إرسال عينات من إشارة كل طرف على فترات زمنية قصيرة غير ملحوظة للأذن البشرية بحيث يمكن إرسالها بشكل متعاقب ومن ثم إعادة فرزها حسب الوجهة.

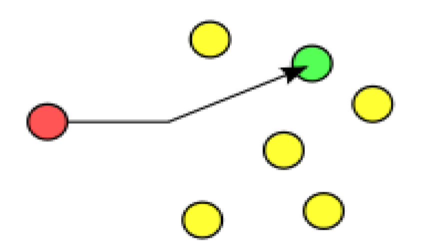
ثانيًا طرق إرسال البيانات في داخل الشبكات

Methods of Sending Data in the Network

توجد أربع طرق لإرسال البيانات داخل الشبكة – برمجيًا - تم إضافة الطريقة الجديد بما تسمى Any Cast والتي تعمل مع IPv6 وهي:

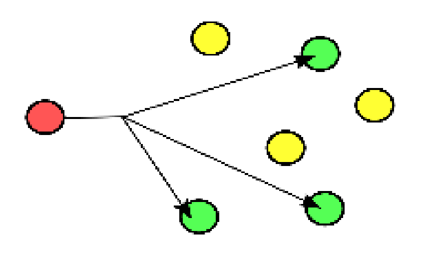
Unicast	هذه العملية تقوم بأخذ البيانات وإرسالها بشكل موحد للجهاز المطلوب فقط لا غير	
Multicast	الإرسال لمجموعة محددة من الأجهزة	
Broadcast	إرسال البيانات لكل الشبكة لجميع الأجهزة تم حذفة في IPv6	
Any cast	آلية لنقل البيانات في الشبكة على شكل أقرب نقطة موجود في IPv6 القدرة على توزيع الترافيك Traffic ما بين السيرفرات وتجنب المشاكل. والأمان أصبح اقوى بكثير	

Unicast



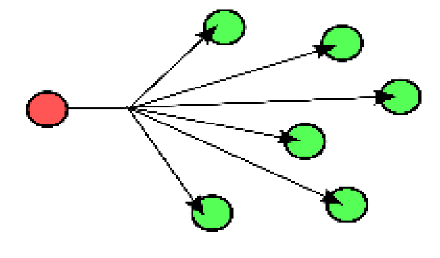
في هذه العملية يتم إرسال البيانات إلى جهاز واحد فقط لا غير، ولا يتم إرسال البيانات لجهاز آخر بمعنى أنه تقوم بعملية الإرسال في اتجاه واحد فقط.

Multicast



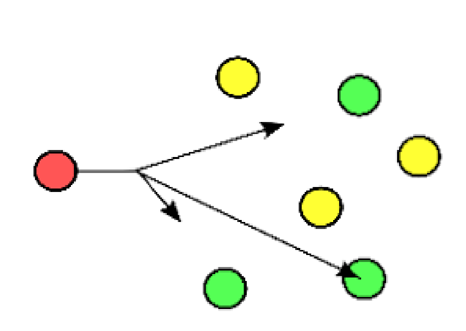
وهنا يكون الإرسال لمجموعة محددة بعينها، ويكون ذلك بتحديد مجموعة محددة من الأجهزة داخل كل أجهزة الشبكة ؛ فمثلاً إذا كان لدينا 51 جهاز و نريد الإرسال لـ 15جهاز هذه هي المجموعة التي تم تحديدها، لتصل البيانات إليها.

Broadcast



إرسال البيانات لجميع الأجهزة المتصلة في الشبكة وهذه العملية تقوم بعمل ثقل في الشبكة وضغط كبير عليها مما ينتج عنه اختناق وحدوث مشاكل في الشبكة .

Any cast



هذه آلية لنقل البيانات في الشبكة على شكل أقرب نقطة؛ فمثلًا عندما يتواجد سيرفران أو خادمان من نفس النوع على سبيل المثال؛ خادم ملفات يتكون من خادمين وعندما يريد أحد المستخدمين الوصول إلى أحد الخوادم تقوم هذه العملية بفحص أقرب نقطة للوصول، ويتم الربط فيزيائيًا، وهذه التقنية أفضل بكثير من تقنية الـ Broadcast.

مميزات الـ Any cast: يوجد عدة مميزات تم وضعها مع هذه التقنية الجديدة:

١. الاعتماد عليه في الشبكة عند وجود أكثر من خادم يقوم بنفس الخدمة.
٢. الأمان أصبح أقوى بكثير مما سبق. مثلما يحدث عند هجوم الـ DDOSعلى السيرفرات سيتم توقف السيرفرات، ولكن مع هذه التقنية أصبح الأمر أصعب.
٣. القدرة على توزيع ال Traffic – مرور البيانات – ما بين السيرفرات عند إرسال واستقبال بيانات.
٤. تجنب المشاكل مثل عند حدوث توقف لسيرفر معين ويوجد سيرفر ثاني يعمل بنفس الخدمة سيتم الانتقال عليه من دون أن يعلم المستخدم إنه تم توقف أحد السيرفرات.

IP، Internet Protocol:



يشير مصطلح IP إلى Internet Protocol أي بروتوكول الإنترنت، وهو مجموعة من القواعد التي تتحكم في البيانات المرسلة عبر جميع الشبكات الحاسوبية –ومن ضمنها شبكة الإنترنت– حيث تعتبر عناوين IP بمثابة الهوية أو المُعرّف الذي يسمح بإرسال وتبادل المعلومات بين الأجهزة الموجودة على الشبكة.

ويستخدم IP مع جميع أنواع الأجهزة المتصلة بالشبكة كالحواسيب الشخصية، أو الهواتف الذكية، أو أجهزة التوجيه، (Router) أو الأجهزة اللوحية، ومهمته الاساسية هي تحديد عنوان تلك الأجهزة لتتمكن من التواصل مع الأجهزة الأخرى على هذه الشبكة .

يحمل كل جهاز عنوان IP مختلف عن باقي الأجهزة، ويمكنك القول إن عنوان بروتوكول الإنترنت مشابه لعنوان منزلك أو رقم هاتفك المحمول، حيث أنه يستخدم لتمييز كل جهاز عن باقي الأجهزة الأخرى الموجودة على الشبكة. وبالتالي كل جهاز متصل بشبكة الإنترنت يجب أن يحمل عنوان IP عام أو عالمي(Global) يكون فريد ومختلف عن عناوين باقي الأجهزة الموجودة حول العالم.

ملحوظة: يجب أن تميز بين عناوين IP الخاصة (Local) التي تستخدم داخل الشبكات المحدودة مثل شبكة المنزل أو المكتب، وعناوين IPالعالمية (Global) أو العامة (Public) التي تستخدم عند الاتصال بشبكة الإنترنت. حيث تتم إدارة عناوين IP العالمية بشكل صارم من قبل مؤسسات متخصصة مثل ICANN و JPNIC بحيث لا تحدث مشاكل مثل تكرار العناوين على الإنترنت.

كيف يتم توزيع IP Address على الأجهزة داخل الشبكة؟

يتكون IP address من 32 bit، ويكون مقسم الى أربع أقسام كل قسم عبارة عن byte أو octet ويتم كتابته بأحد الأساليب التالية:

١. استخدام النظام الثنائي ويكون كل قسم مفصول عن الآخر بنقطة مثل :١٧٢.١٦.٣٠.٥٦.
٢. باستخدام النظام العشري مثل AC101E38 : ويستخدم في سجل النظام.Windows Registry

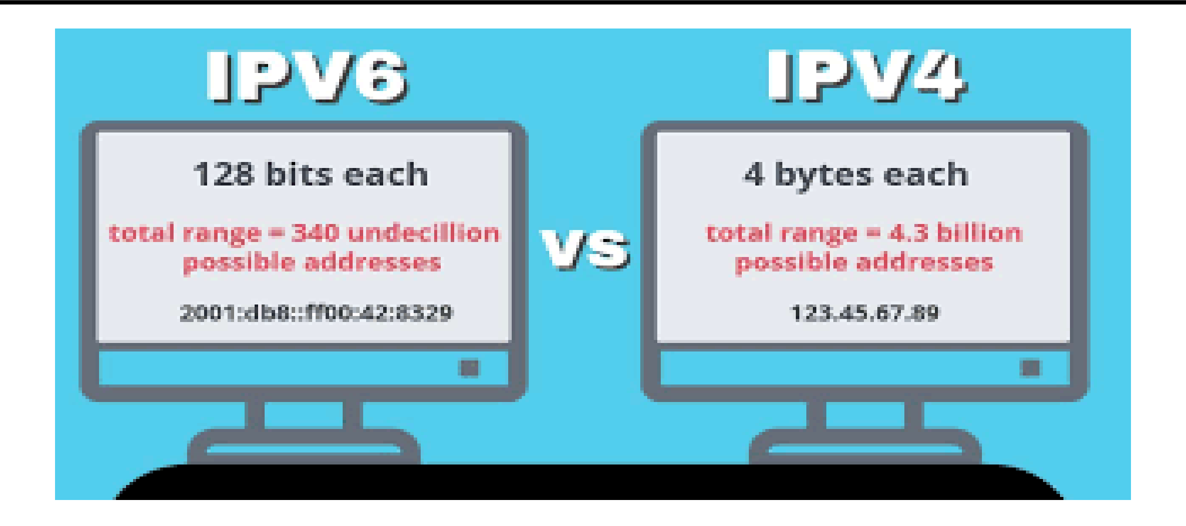
كل الأساليب السابقة تستخدم لعرض نفس العنوان ولكن بطرق مختلفة والأكثر استخداما بينها هو الأسلوب الأول وهو شبيه بأرقام الهواتف حيث يبدأ برقم البلد ثم المنطقة ثم رقم الهاتف الخاص.

مثال توضيحي:

تعتمد شركات الاتصالات على أرقام الهواتف لإجراء اتصال هاتفي، فنحن لا نستخدم الأسماء ولا المواقع للاتصال بالأشخاص عبر الهاتف نحن فقط نستخدم رقم الشخص بعض النظر عن اسمه أو موقعه، ويتولى الحاسب بعد ذلك ربطنا بالشخص المطلوب، بالمثل في عالم الإنترنت كل جهاز يرتبط بشبكة إنترنت يجب أن يحصل على رقم يميزه عن غيره، كل موقع وكل صفحة على الإنترنت يجب أن يكون لها رقم خاص يميزها عن غيرها، هذا الرقم المميز لكل متصل بالإنترنت وكل موقع انترنت يسمى (IP Address).

ملحوظة هامة:

عليك أن تعرف أن جميع الأجهزة المتصلة بنفس الشبكة يشتركون في أن عناوين IP لكل منهم تحتوي على عنوان نفس الشبكة مثلا لنفترض وجود جهازين في الشبكة أحدهما له العنوان١٩٢.١٦٨.١.٢ و الآخر لديه العنوان١٩٢.١٦٨.١.٣ نلاحظ أنهما يشتركان في نفس عنوان الشبكة و هو١٩٢.١٦٨.١ ، و لكن يكون لكل منهما عنوانه الخاص و يطلق عليه node address أو host address وهو في مثالنا للجهاز الأول٢ و للجهاز الثاني٣.



يشير مصطلحي IPv4 و IPv6 إلى معايير عنوان IP التي تحدد كيفية تخصيص عنوان IP وما يمكن أن تشير إليه، حيث أن أرقام ٤ أو ٦ هي أرقام الإصدارات، كما أنه توجد بعض الاختلافات الأساسية بينهما، لكنها تمثل كل من عناوينIP .

IPv4 بروتوكول الإنترنت الإصدار الرابع

هو الإصدار الحالي الذي نستخدمه حاليا في الاتصال بالإنترنت، وهو يسمى الإصدار الرابع؛ ليس لأنه يتكون من أربع خانات كما قد يظن البعض بل لأنه هو الإصدار الرابع من Internet Protocol IP) (Version 4، وهو الإصدار الذي يتعامل به العالم جميعاً حاليًا، ويتكون من ٣٢ بت تتوزع على أربع خانات كل خانة من الخانات الأربع يمكن أن تأخذ الأرقام من ٠ إلى ٢٥٥؛ مع العلم بأنه يوجد أرقام محجوزة أو ممنوعة من الاستخدام.



IP addresses are a **unique identifier assigned to internet-connected devices** and they're required for your device to access the internet.

ويمكننا أن معرفة عدد الأرقام المختلفة التي يمكن الحصول عليها فهي حاصل رقم (2^{32}) حيث يمكن توزيع (4,294,967,296) رقم، أي ما يقارب ٤ مليارات وثلث المليار IP حول العالم، ولقد كان هذه العدد الضخم في بداية ظهور الإنترنت كبير جدا، ولكن مع توسع الإنترنت وزيادة عدد المستخدمين وزيادة عدد مواقع وصفحات الإنترنت أصبحت هذه الأرقام لا تكفي المستقبل القريب مع التطور الزيادة السريعة لمستخدمي الحاسب .

المقطع هو الخانة هو

الـ IP Address يُكتب على شكل 4 مقاطع؛

كل مقطع يسمى Octet ويفصل بين كل Octet والثاني بـ '.'

مثال: 100.90.55.10

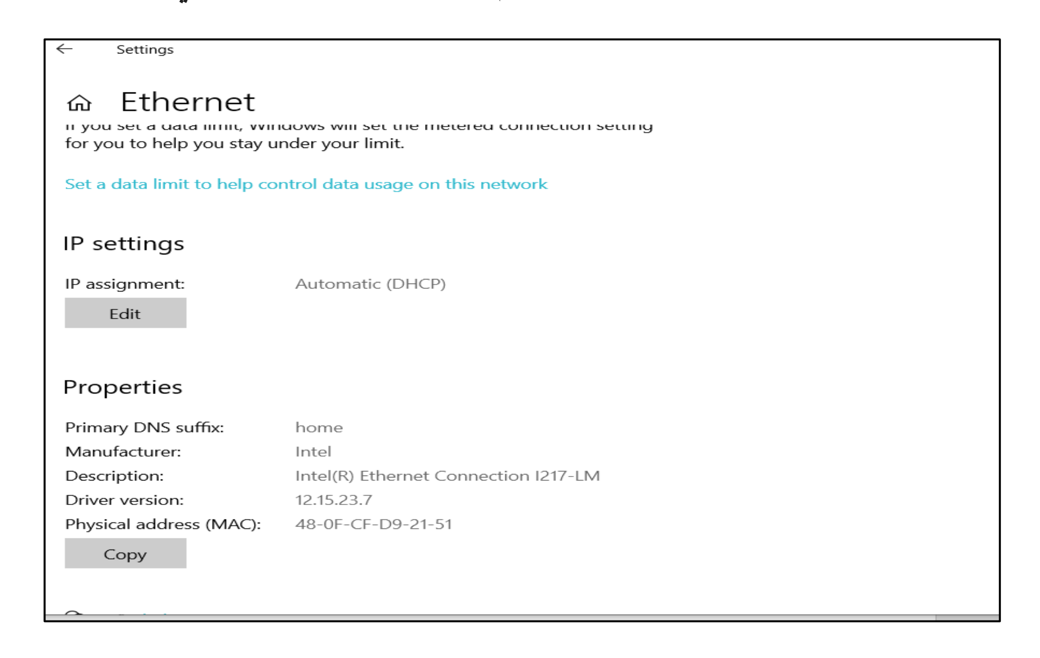
لتمكين DHCP أو تغيير إعدادات TCP/IP الأخرى:

١. حدد **Start** ثم**Setting** ثم Network & Internet.

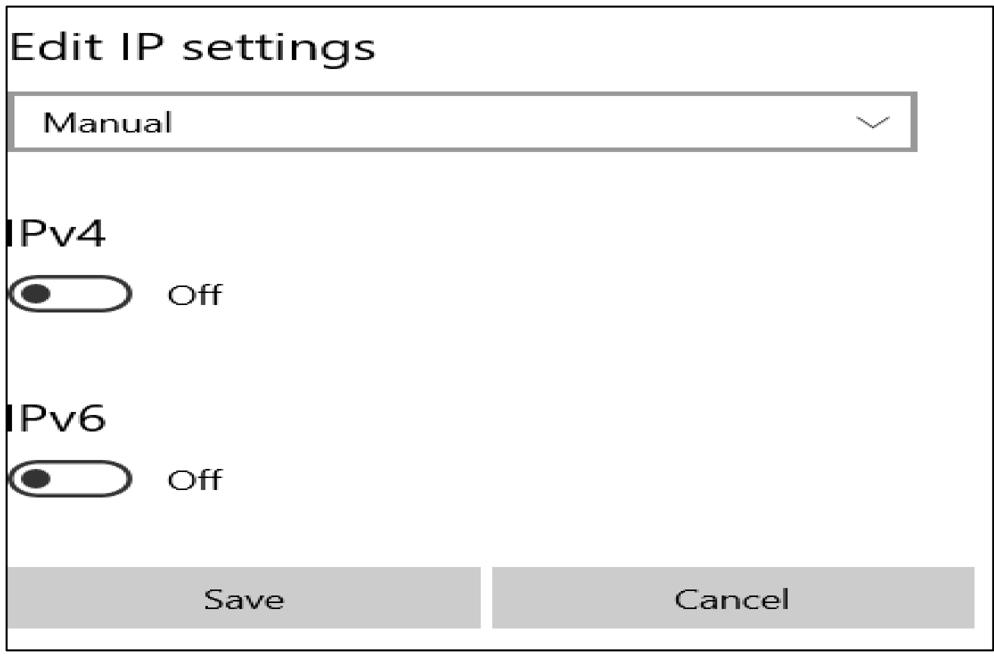
٢. قم بتنفيذ أحد الإجراءين التاليين:

أ. بالنسبة لشبكةWi-Fi ، حدد **Wi-Fi <** **إدارة الشبكات المعروفة**. اختر الشبكة التي تريد تغيير الإعدادات لها.

ب. بالنسبة لشبكةEthernet ، حدد **Ethernet**، ثم حدد شبكة Ethernet التي تتصل بها.



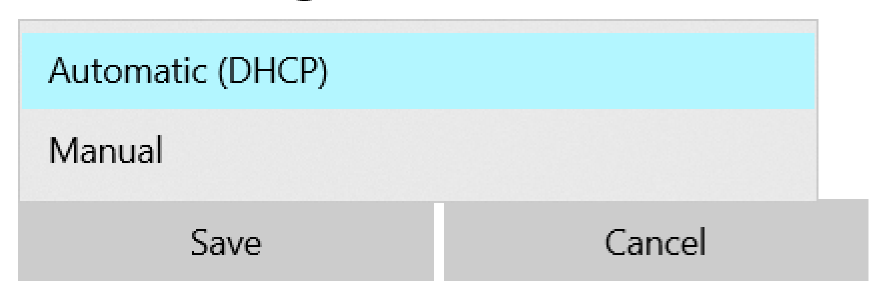
٣. إلى جانب **تعيين IP**، حدد "**تحرير**".



٤. ضمن **تحرير إعدادات IP للشبكة** أو **تحرير إعدادات IP**، حدد **تلقائي (DHCP)** أو **يدوي**.

- **لتحديد إعدادات IPv4 يدويًا**

١. ضمن "**تحرير إعدادات IP للشبكة**" أو "**تحرير إعدادات IP**"، اختر "**يدوي**"، ثم قم بتشغيل **IPv4**.



٢. لتحديد عنوان IP، في **عنوان IP وقناع الشبكة الفرعية** ومربعات **البوابة**، اكتب إعدادات عنوان IP.

٣. لتحديد عنوان خادم DNS، في خانتي الاختيار **DNS المفضل** و **DNS البديل**، اكتب عناوين خوادم DNS الأساسية والثانوية.

٤. لتحديد ما إذا كنت تريد استخدام اتصال مشفر DNS عبر HTTPS أو اتصال غير مشفر بخادم DNSأو الخوادم التي تحددها، بالنسبة إلى **DNSعبرHTTPS** ، اختر الإعداد الذي تريده.

٥. **إيقاف التشغيل**: سيتم إرسال كافة استعلامات DNS إلى خادم DNS غير مشفر في نص عادي عبر HTTP.

في (قالب تلقائي): سيتم تشفير استعلامات DNS وإرسالها إلى خادم DNS عبر HTTPS. ستستخدم استعلامات DNS الإعدادات الافتراضية للقالب التلقائي أو تحاول اكتشافها تلقائيا.

في (قالب يدوي): سيتم تشفير استعلامات DNS وإرسالها إلى خادم DNS عبر HTTPS. سيستخدمون الإعدادات التي تدخلها في **مربع قالب DNS عبرHTTPS** .

IPv4
On
IP address
Subnet prefix length
Gateway
Preferred DNS
Alternate DNS
Save Cancel

إذا كنت تستخدم DNS عبر HTTPS(قالب تلقائي أو يدوي)، فقم بتشغيل **النص العادي** أو إيقاف تشغيله:

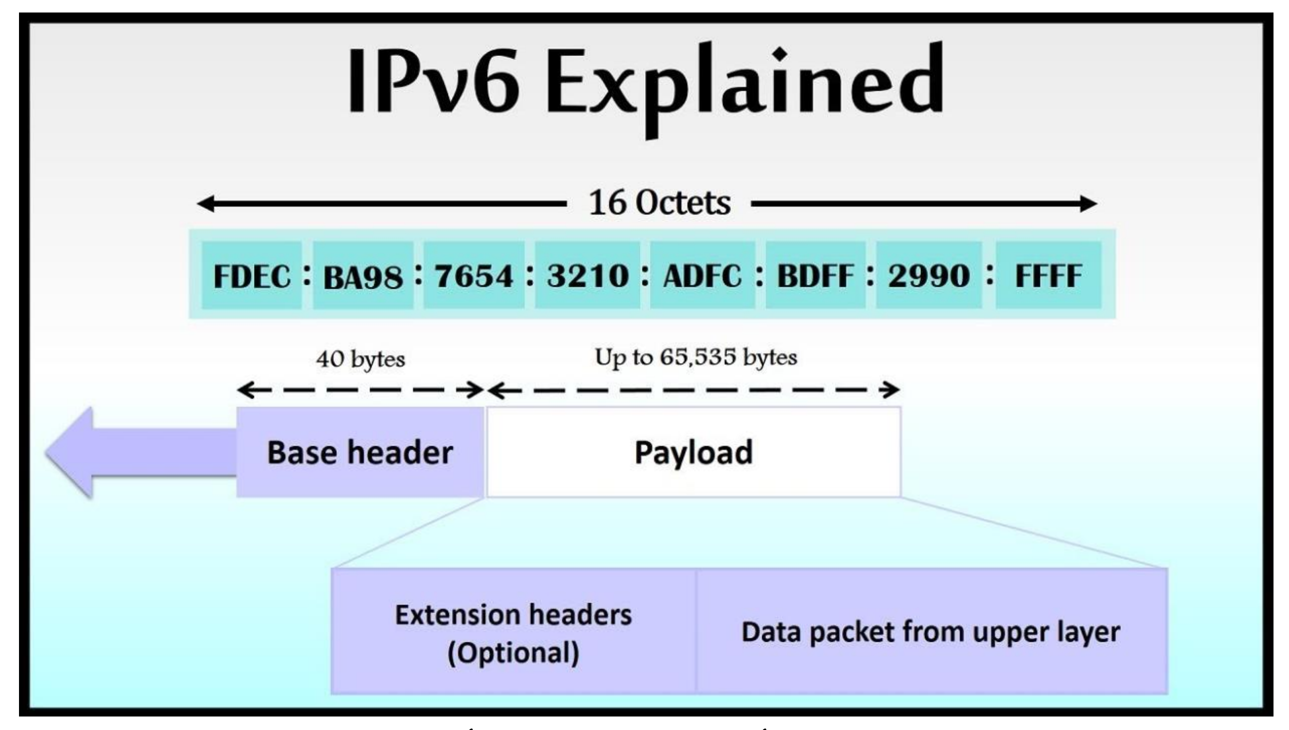
أ. عند تشغيله، سيتم إرسال استعلام DNS بدون تشفير إذا تعذر إرسالها عبر HTTPS.

ب. عند إيقاف تشغيله، لن يتم إرسال استعلام DNS إذا تعذر إرساله عبر HTTPS.

IPv6 بروتوكول الإنترنت الإصدار السادس

بروتوكول الإنترنت الإصدار السّادس Internet Protocol Version 6 هو تطوير لبروتوكول الانترنت الإصدار الرّابع IP. IPv6 يستخدم ١٢٨ بت في ثمان خانات ، وهي تتسع لأرقام لا حصر لها من العناوين وذلك لتفادي مشكلة IPv4، كما أنها تستخدم الحروف والأرقام معاً وليس الأرقام فقط أي تستخدم الأرقام بالنظام العشري Decimal وليس الثنائي Binary؛ والمكونة من ١٦ حرف ورقم ، وهي كالتالي (0.1.2.3.4.5.6.7.8.9.A.B.C.D.E.F) كما هو موضح بالشكل أعلاه.

ويتكون من ثمان خانات بدلًا من أربع كما هو في البرتوكول IPv4؛ حيث يحوي أرقاما وحروفا وهي المستخدمة في النظام العددي العشري بدلا من الأرقام الثنائية، فقط كما هو الحال في البروتوكول IPv4. إذا



يمكننا الحصول على عدد هائل جدا من أرقام IP، حيث تستطيع أن توزع من خلالها ٦ تريليون IP حول العالم، أو ما يساوي (2^{128}) والذي يعطي ناتجه رقما مكون من ٣٩ خانة. مما يوضح العدد الهائل من ال IP التي يمكن الحصول عليها مما يعني أنه يمكن إعطاء IP فريد لكل سنتيمتر واحد على الأرض أو ما يعادل ١٠٠٠٠ IP لكل متر على الأرض . فهل يمكن لمتر واحد أن يحوي ١٠٠٠٠ جهاز ويعود سبب تلك الزيادة الهائلة بين الإصدارين لبنية IP الجديد التي تتكون من ١٢٨ بت للإصدار IPv6 وتتكون من أرقام عشرية بدلا من ثنائية في الإصدار IPv4.

▪ **لتحديد إعدادات IPv6 يدويًا**

١. ضمن "تحرير إعدادات IP للشبكة "أو "تحرير إعدادات"IP ، اختر "يدوي"، ثم قم بتشغيل IPv6. كما ذكرنا في IPV4 أعلاه.

٢. لتحديد عنوانIP ، في عنوان IP وطول بادئة الشبكة الفرعية ومربعات البوابة، اكتب إعدادات عناوين IP.

٣. لتحديد عنوان خادمDNS ، في خانتي الاختيار DNSالمفضل و DNSالبديل، اكتب عناوين خوادم DNSالأساسية والثانوية .

٤. لتحديد ما إذا كنت تريد استخدام اتصال مشفر (DNS عبر HTTPS) أو اتصال غير مشفر بخادم DNSأو الخوادم التي تحددها، بالنسبة إلى DNS **عبرHTTPS** ، اختر الإعداد الذي تريده

٥. **إيقاف التشغيل**: سيتم إرسال كافة استعلامات DNS إلى خادم DNS غير مشفر في نص عادي عبر .HTTP

أ. **في (قالب تلقائي):** سيتم تشفير استعلامات DNS وإرسالها إلى خادم DNS عبر .HTTPS ستستخدم استعلامات DNS الإعدادات الافتراضية للقالب التلقائي أو تحاول اكتشافها تلقائيا.

ب. **في (قالب يدوي):** سيتم تشفير استعلامات DNS وإرسالها إلى خادم DNS عبر .HTTPS سيستخدمون الإعدادات التي تدخلها في **مربع قالب DNSعبر.HTTPS**

IPv6
On
IP address
Subnet prefix length
Gateway
Preferred DNS
Alternate DNS
Save Cancel

٦. إذا كنت تستخدم DNS عبر HTTPS (قالب تلقائي أو يدوي)، فقم بتشغيل النص العادي أو إيقاف تشغيله:

أ. عند تشغيله، سيتم إرسال استعلام DNS بدون تشفير إذا تعذر إرساله عبر .HTTPS

ب. عند إيقاف تشغيله، لن يتم إرسال استعلام DNS إذا تعذر إرساله عبر .HTTPS

٧. عند تحديد التلقائية(DHCP) ، يتم تعيين إعدادات عنوان IP وإعداد عنوان خادم DNS تلقائيًا بالموجه أو نقطة الوصول الأخرى (مستحسن).

٨. عند تحديد يدوي، يمكنك يدويًا تعيين إعدادات عنوان IP الخاص بك وعنوان خادم.DNS

٩. عندما تنتهي، حدد حفظ.

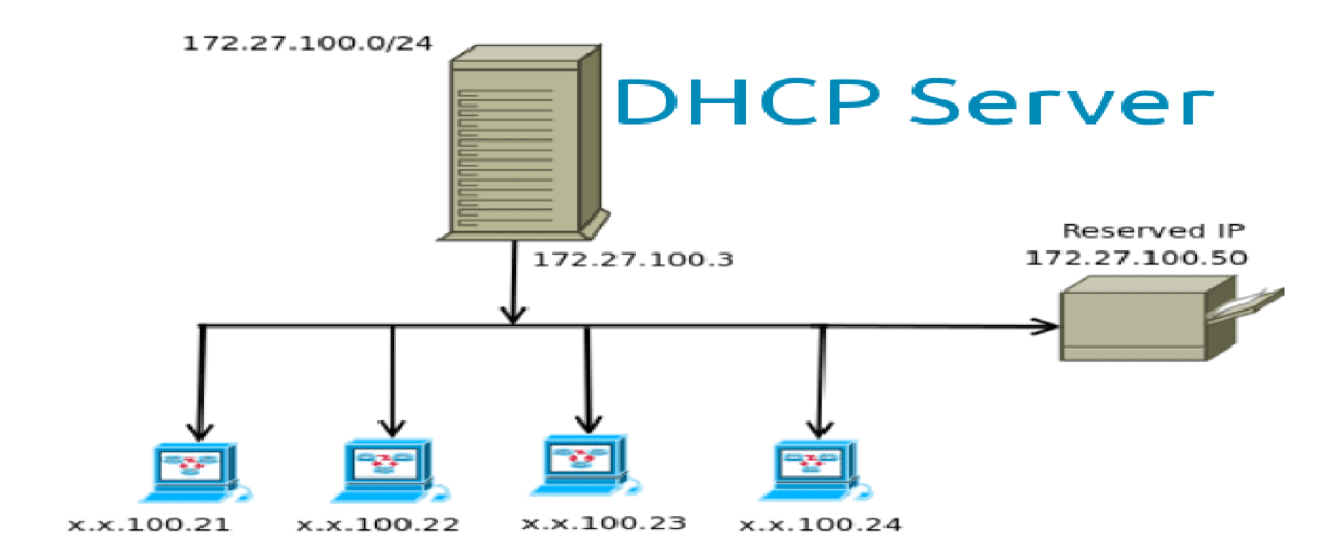
يوضح الجدول التالي أهم الفروق والاختلافات بين IPv4، و IPv6

المعيار	IPv4	IPv6
الإصدار	الرابع من بروتوكول الإنترنت	السادس من بروتوكول الإنترنت
تاريخ الإصدار	1981	1999
أرقام الحِزَم	32Bit	128Bit
عدد الخانات في الحِزمة	4 تأخذ الأرقام من صفر إلى ٢٥٥ مكتوبة بالنظام الثنائي	8 تأخذ أرقام عشوائية مكتوبة بالنظام العشري
شكل المقاطع	2^32=4,294,697,296	2^128= 340,282,366,920,938,643,374,607,431,768,211,456
مدى رأس ال Packet	عشوائي (20Byte)	محدد (40Byte)
اختبار رأس ال Packet	مطلوب لقياس الأخطاء الرأس	يتم معرفته من رأس الحزمة
العنونة	DHCP	SLAAC/DHCPv6
حماية ال IP	اختياري	إلزامي
أقل حجم للنقل	576 Byte مقسمة على حِزم	1028 Byte
قوة ال IP	غير عملي	عملي

لكل جهاز على شبكة لابد من عنوان IP Address سواء كان هذا الجهاز هو جهاز كمبيوتر أو هاتف ذكي أو طابعات أو كاميرات مراقبة وغيرها، فكل تلك الأجهزة تحصل على عنوان IP Address خاص بها وقد تعرفنا على كيفية إضافة ipيدويًا، ولكن كيف تحصل تلك الأجهزة على عنوان IP بشكل تلقائي بمجرد توصيلها على الشبكة؟ وكيف يختلف عنوان IP هذا من جهاز لآخر؟

:DHCP

DHCP هو اختصار لكلمة Dynamic Host Configuration Protocol هذا البروتوكول هو المسئول عن تعيين عنوان IP Address لكل جهاز يتم توصيله علي الشبكة بشكل تلقائي دون تدخل منك وأيضاً يقوم بتعيين بعض الإعدادات لكل جهاز متصل بالشبكة لكي تستطيع التحكم والسيطرة فيها علي تلك الأجهزة ليصبح الأمر أسهل عليك وأكثر تحكماً.



وظيفة بروتوكول.DHCP

بالإضافة إلى الإدارة المبسطة، يوفر استخدام خادم DHCP مزايا أخرى عديدة. ومن أهمها:

١. تكوين IP دقيق.

يجب أن تكون معلمات تكوين عنوان IP دقيقة وعند التعامل مع مدخلات مثل "١٩٢.١٦٨.١٥٩.٣"، من السهل ارتكاب الأخطاء. عادةً ما يكون من الصعب جداً استكشاف الأخطاء وإصلاحها، كما أن استخدام خادم DHCP يقلل من هذه المخاطر.

٢. تقليل تعارض عناوين.IP

يجب أن يكون لكل جهاز متصل عنوان .IP ومع ذلك، لا يمكن استخدام كل عنوان إلا مرة واحدة. وسيؤدي العنوان المكرر إلى تعارض حيث لا يمكن توصيل أحد الجهازين أو كليهما. يمكن أن يحدث هذا عندما يتم تعيين العناوين بشكل يدوي، خاصةً عند وجود عدد كبير من نقاط النهاية التي تتصل فقط بشكل دوري، مثل الأجهزة المحمولة. يضمن استخدام DHCP استخدام كل عنوان مرة واحدة فقط.

٣. التأكد من إتمام عنوان الموقع لكل جهاز داخل الشبكة.

بدون بروتوكولDHCP ، سيحتاج مسؤولو الشبكة إلى تعيين العناوين وإبطالها بشكل يدوي. يمكن أن يكون تتبع الجهاز الذي يحتوي على العنوان أمراً عبثياً لأنه يكاد يكون من المستحيل فهم متى تتطلب الأجهزة الوصول إلى الشبكة ومتى تغادر. يسمح بروتوكول DHCP بأتمتة هذا الأمر وجعله مركزياً حتى يتمكن محترفو الشبكة من إدارة جميع المواقع من موقع واحد.

٤. إدارة التغيير الفعالة.

يجعل استخدام DHCP من السهل جداً تغيير العناوين أو النطاقات أو نقاط النهاية. على سبيل المثال، قد ترغب إحدى المؤسسات في تغيير نظام عناوين IP الخاص بها من نطاق إلى آخر. يتم تكوين خادم DHCP بالمعلومات الجديدة، وسيتم نشر المعلومات إلى نقاط النهاية الجديدة. وبالمثل، إذا تمت ترقية جهاز الشبكة واستبداله، فلا يلزم تكوين شبكة في هذه الحالة.

DNS نظام أسماء النطاقات

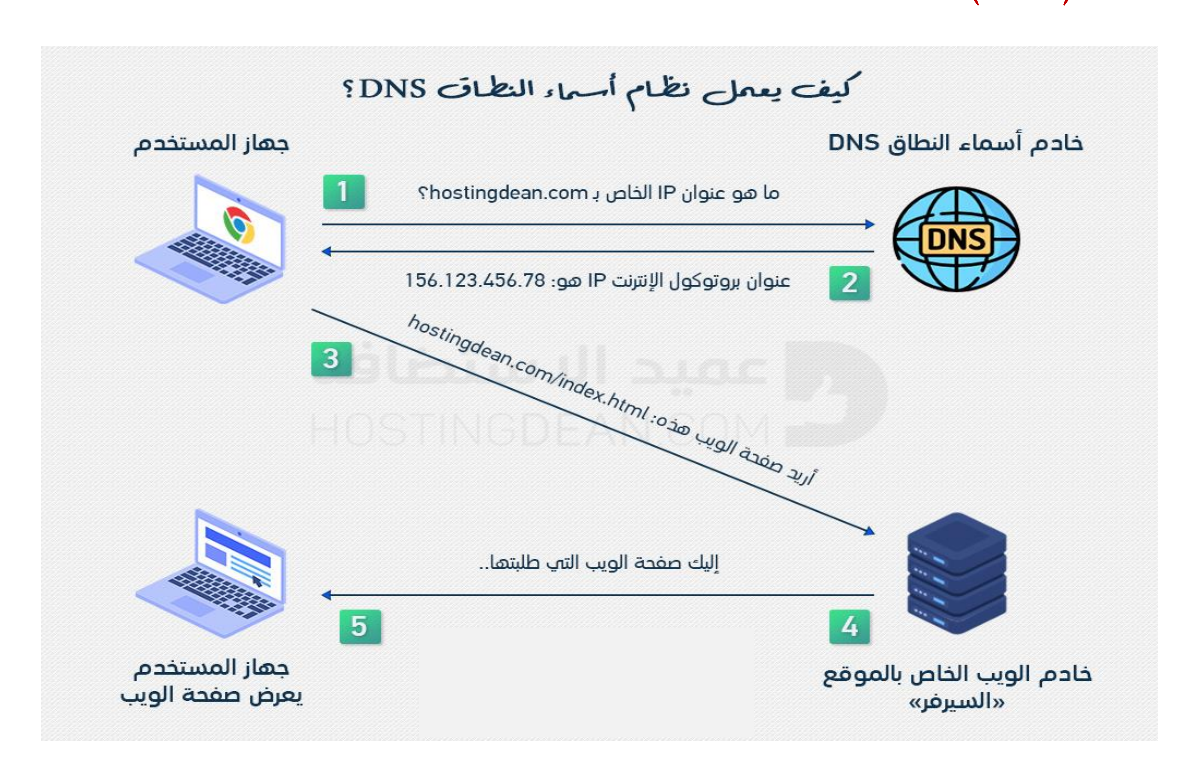


ما هو DNS؟

هو اختصار لجملة(Domain Name System) ، كما نعلم لا يمكن الوصول الى الموقع الفيزيائي للجهاز الذي نحاول الاتصال به عن طريق اسم الموقع hostname فقط، فجميع الاتصالات تتم باستخدام عناوين IP، لذا فنحن بحاجة لخدمة.DNS

وخادم DNS هو جهاز يربط بين اسم الموقع hostname وعنوان IP للجهاز المراد الوصول إليه الذي يستضيف هذا الموقع. وهو نظام يخزّن عناوين الصفحات الإلكترونية للوصول إليها، فهو بمثابة دليل عناوين الصفحات على شبكة الإنترنت، أي أن ال (DNS) مسؤولٌ عن ترجمة اسم الموقع من حروف إلى أرقام عناوين ال (IP) الصحيحة لتلك المواقع ومن ثمّ استخدام هذه العناوين للتواصل مع الخوادم الأصليّة(CDN) للوصول إلى معلومات موقع الويب.

كيف يعمل (DNS)؟



عند قيام المستخدم بكتابة اسم الموقع على سبيل المثال (www.example.com) في متصفحّه يأتي دور ال DNS كالتالي:

٥. يرسل المتصّفح اسم الموقع الذي كتبه المستخدم عبر مزوّد شبكة الإنترنت الخاص به (ISP) إلى خادم (DNS).

٦. يرسل خادم (DNS) الاستعلام الكامل إلى خادم بمستوى الأعلى (TLD) والتي تحتوي أيضاً على (com) و (net) و(org) .

٧. يعيد محلل (DNS) وهو (Resolver) استقبال العنوان الكامل.

٨. يرجع محلل DNS عنوان (IP) الخاص بالمجال المطلوب إلى مستعرض الويب المطلوب.

٩. يرسل المتصفح طلب (HTTPS) إلى عنوان (IP) المستهدف.

١٠. يعيد الخادم (DNS) الذي يحمل هذا العنوان صفحة الويب، والتي يتم عرضها في متصفح المستخدم.

ما هي مكوّنات خادم(DNS) ؟

يتكوّن نظام خادم (DNS) من المكوّنات الآتية:

١. **الخادم(Server)** : الذي يقوم بإعادة المعلومات المتعلّقة باسم النطاق.

٢. **اسم النطاق(Domain Name)** : وهو الذي يقوم المستخدم بإدخاله لتحويله إلى أرقام يفهمها الحاسوب للوصول إليه.

٣. **المحلل(Resolver) :** وهو يرجع المعلومات إلى الخادم الأساسي للنظام.

ما هي أنواع خوادم(DNS) ؟

١. الخادم المركزي Root DNS Server

الخوادم المركزية هي التي لديها عناوين جميع خوادم نطاق المستوى الأعلى Top Level Domain TLD Server، إذ يصل الطلب أولًا للخوادم المركزية لنظام DNS في رحلته للحصول على عنوان IP لاسم الموقع المطلوب.

ويوجد ١٣ خادمًا مركزيًا منتشرةً حول العالم حتى تاريخ العام ٢٠١٦، وهذا لا يعني وجود ١٣ جهاز فقط حول العالم للتعامل مع الطلبات الهائلة في كل العالم، إذ يوجد عدة خوادم لدى مزودي خدمات الإنترنت ISPs المحليين للاستجابة لهذه الطلبات.

وتقوم عدة منظمات بإدارة الخوادم المركزية لنظام DNS وهنا قائمة بها:

List of Root Servers

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

٢. خادم نطاق المستوى الأعلى Top Level Domain TLD Server

يُصنَّف هذا النوع من الخوادم نسبةً الى نطاقات المستوى الأعلى مثل (.com) المخصص للشركات و (.org)للمنظمات الغير ربحية و(.au) نسبة لدولة أستراليا (علمًا أن لكل دولة نطاق خاص بها) وغيرها.

وعادةً ما تكون خوادم المستوى الأعلى وجهة رسائل الطلب بعد خادم DNS المركزي، ويُخزّن فيها سجلٌ مخصصٌ لنطاق TLD لاسم الموقع المطلوب. فمثلًا إذا طلبنا عنوان IP للموقع aliens-sci.com عندها ستذهب رسالة الطلب الى خوادم TLD الخاصة بالنطاق .com يقوم خادم النطاق TLD عندها بإرسال عنوان خادم DNS الموثّق Authoritative DNS server إلى المُقرّر .DNS Resolver

Nameserver
ns6.wixdns.net
ns7.wixdns.net
ns1.digitalocean.com
ns2.digitalocean.com
ns3.digitalocean.com

(خوادم TLD مشيرة الى خوادم الأسماء الموثّقة)Authoritative Name servers

٣. الخادم التكراريّ: (Recursive DNS Server)

يتمثّل عمل الخادم التكراري في الاستجابة لطلب المستخدم ويعيد عنوان (IP) لاسم العنوان المطلوب الذي كتبه المستخدم، من خلال إجراء سلسلة من الأوامر حتى يصل إلى الخادم (DNS) الرئيسي للمجال المطلوب.

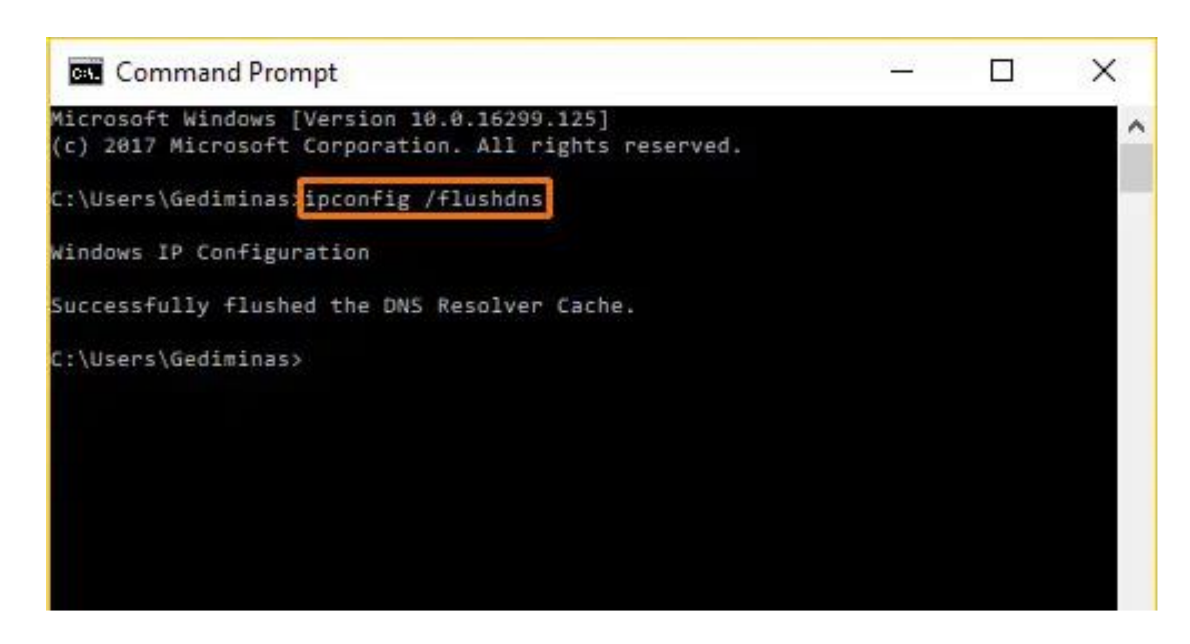
٤. الخادم الموثوق (Authoritative DNS Server)

يتمثل عمل الخادم الموثوق بالاحتفاظ بسجل المجال المطلوب من خلال عمليات محدّثة، ممّا يسمح للمسؤولين بإدارة أسماء (DNS) العامّة والخاصّة بهم، حيث يُعتبر الخادم الموثوق هو المصدر النهائيّ لحقيقة المعلومات الخاصّة بخادم(DNS) ، بالإضافة إلى أنّه المسؤول عن توفير معلومات عنوان (IP) للنطاق مرّة أخرى إلى خادم (DNS) التكراريّ المطلوب.

والآن كيف نتحكم بال DNS على نظام التشغيل Widows10؟

إذا حدثت مشكلة في الوصول إلى موقع ويب، وكان السبب في ذلك هو وجود مشكلة فيDNS ، فإن الخطوة الأولى هي حذف هذه المعلومات حتى يتم تحديثDNS . حيث أن DNS المواقع لديها تعليمات حول مسح نظام أسماء النطاقات لكل إصدار من أنظمة تشغيلWindows ، بالإضافة إلى نظامي التشغيل MacOS وLinux. ويمكن مسحDNS على ويندوز باتباع الخطوات التالية:

من خلال موجه الأوامر CMD باستخدام الأمر .ipconfig / flushdns



وإذا لم يؤدي مسح ذاكرة التخزين المؤقت لنظام أسماء النطاقات على جهاز الكمبيوتر الخاص بك إلى حل مشكلة DNS لديك، فعليك بالتأكيد محاولة إعادة تشغيل جهاز التوجيه – الراوتر – الخاص بك لمسح ذاكرة التخزين المؤقت لنظام أسماء النطاقات.

أيضًا يمكن تغيير خوادم DNS على الكمبيوتر –الويندوز–

نظرًا لأن خوادم DNS هي أحيانًا تتسبب في أنواع معينة من مشاكل الإنترنت، فقد يكون تغيير خوادم DNS خطوة جيدة لاستكشاف الأخطاء وإصلاحها. فعند تغيير خوادم DNS في Windows ، يمكنك تغيير الخوادم التي يستخدمها Windows لترجمة أسماء النطاقات (مثل www.estafed1.com) إلى عناوين IP) مثل ٢٠٨.١٨٥.١٢٧.٤٠).

نظرًا لأن معظم أجهزة الكمبيوتر وأجهزة الهواتف أيضًا تتصل بشبكة محلية عبر DHCP ، فمن المحتمل أن هناك بالفعل خوادم DNS مكونة تلقائيًا في Windows نيابة عنك.

ما ستفعله هنا هو تجاوز خوادم DNS التلقائية، وتبديلها بخوادم DNS أخرى من اختيارك.

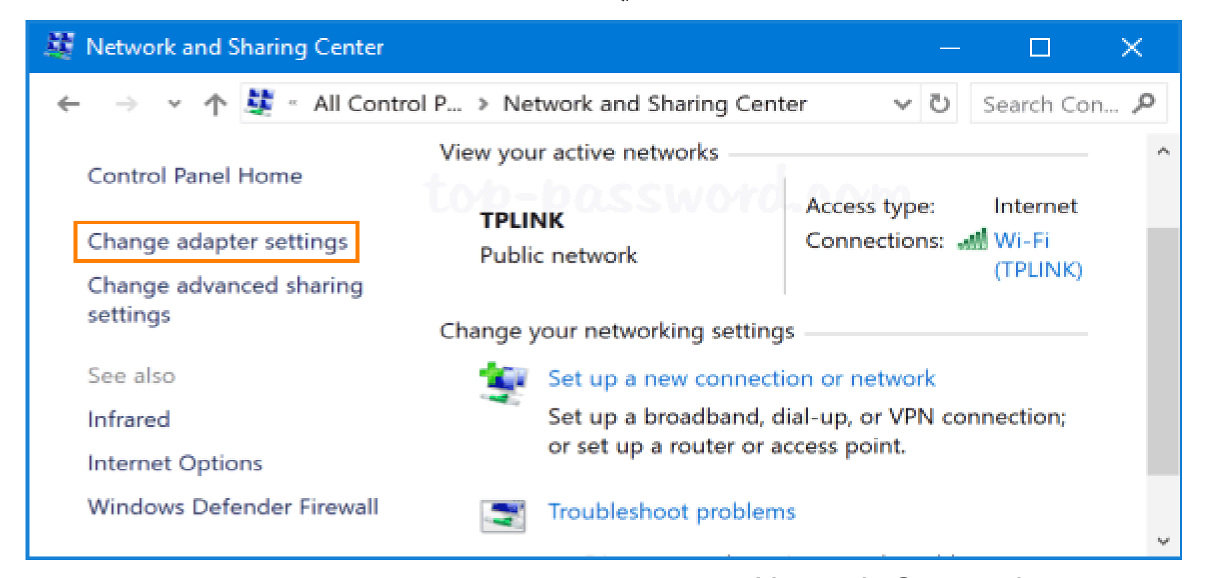
فيما يلي الخطوات المطلوبة لتغيير خوادم DNS التي يستخدمها Windows10 .

١. قم بفتح لوحة التحكم .**Control Panel**

٢. قم بتحديد الخيار Network and Internet.

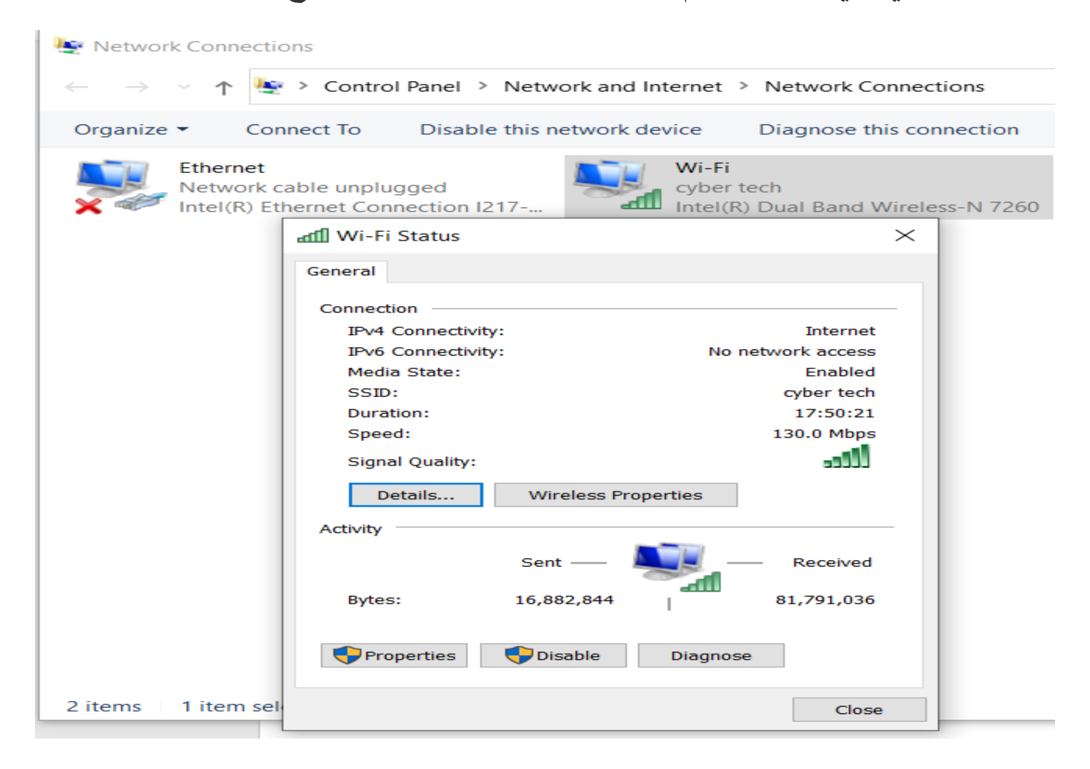
٣. ومن نافذة الشبكة والإنترنت المفتوحة، انقر على خيار Network and Sharing Center.

٤. لآن بعد أن تم فتح نافذة مركز الشبكة والمشاركةNetwork and Sharing Center ، انقر فوق الأمر Change adapter settings، الموجود في الجانب الأيسر



٥. من شاشة Network Connections الجديدة هذه، حدد بالماوس موقع اتصال الشبكة الذي تريد تغيير خوادم DNS له.

٦. افتح اتصال الشبكة الذي تريد تغيير خوادم DNS له من خلال النقر المزدوج على الأيقونة الخاصة به.

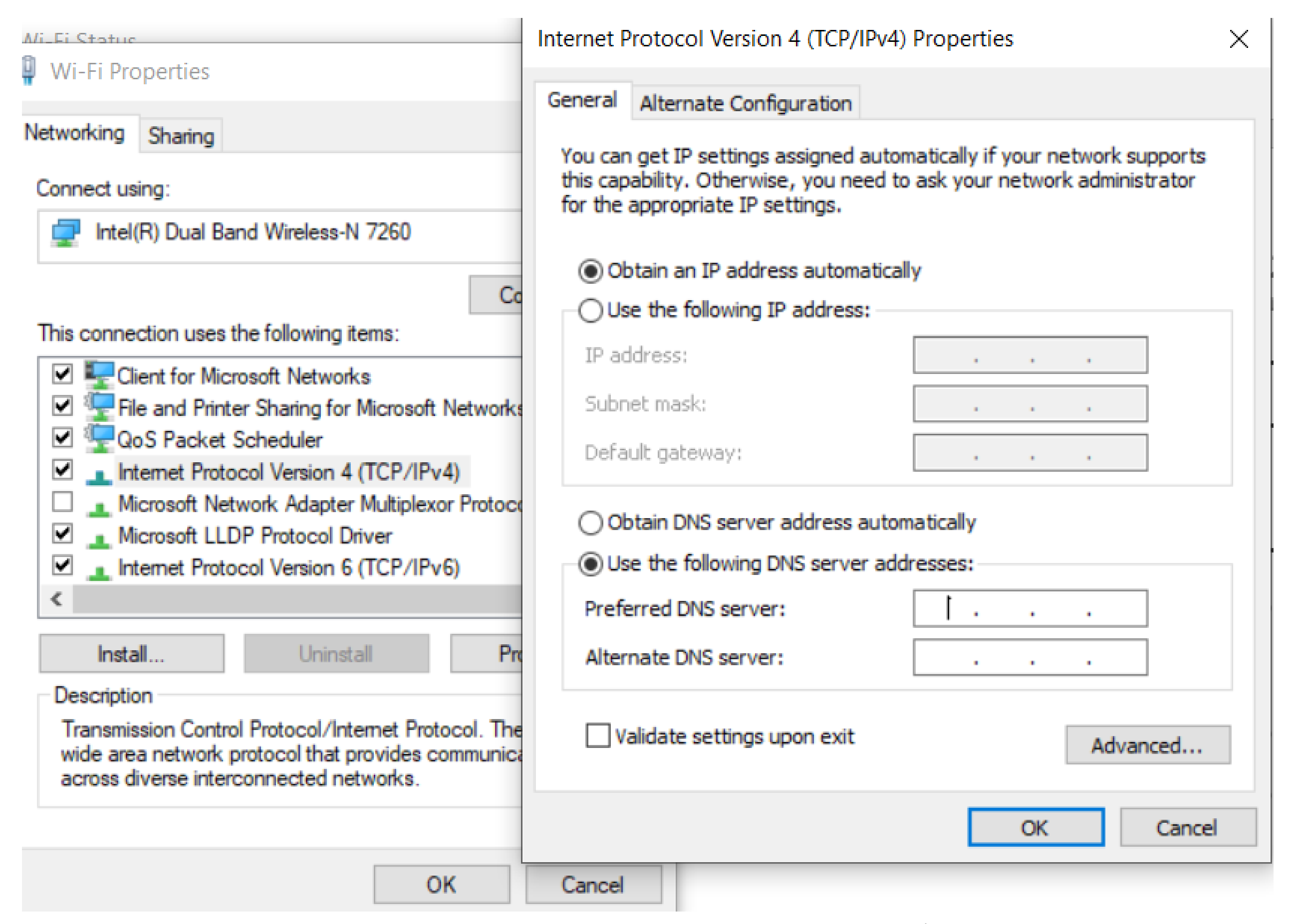


٧. انقر فوق خصائص "Properties" في نافذة الحالة الخاصة بالاتصال المفتوحة الآن.

٨. ومن نافذة خصائص الاتصال التي تظهر، انقر على خيار (Internet Protocol Version 4) TCP/IPv4.

٩. اضغط أو انقر فوق الزر خصائص "Properties" أسفل القائمة.

١٠. من نافذة الخصائص التي تم فتحها، انقر على الخيار Use the following DNS server addresses.



١١. في المساحات الفارغة، أدخل عنوان IP لخادم DNS المفضل **Preferred DNS server** ، بالإضافة إلى خادم DNS بديل **Alternate DNS server.**

١٢. وأخيرًا، اضغط على زر موافق OK .

ملحوظة: يمكنك إدخال خادم DNS المفضل فقط **Preferred DNS server** ، ولا يشترط عليك إدخال خادم DNS البديل **Secondary DNS Server** ، ولكن من الأفضل إضافة كليهما، وذلك في حالة حدوث خطأ في خادم DNS المفضل، يتم الانتقال إلى خادم DNS البديل.

التطبيق الأول؛ إعدادات الربط الشبكي:

يقوم الطالب بتطبيق وضع الإعدادات الخاصة بكارت الشبكة NIC من خلال نظام التشغيل ويندوز Windows أو باستخدام برنامج Packet tracer كما بالخطوات الاتية: -

باستخدام ويندوز ١٠

١. قم بفتح لوحة التحكم **Control Panel.**

٢. قم بتحديد الخيار Network and Internet.

٣. ومن نافذة الشبكة والإنترنت المفتوحة، انقر على خيار Network and Sharing Center.

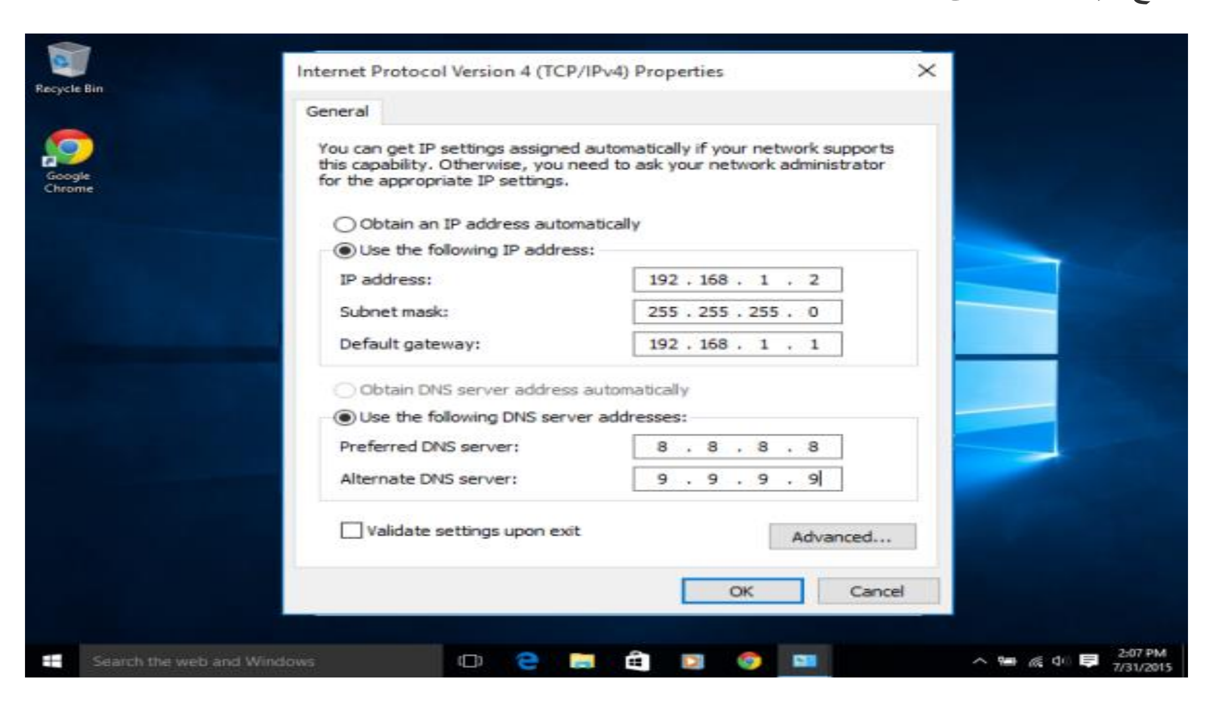
٤. لآن بعد أن تم فتح نافذة مركز الشبكة والمشاركةNetwork and Sharing Center ، انقر فوق الأمرChange adapter settings، الموجود في الجانب الأيسر

٥. من شاشة Network Connections انقر فوق خصائص "Properties" في نافذة الحالة الخاصة بالاتصال المفتوحة الآن.

٦. ومن نافذة خصائص الاتصال التي ظهرت، انقر على خيار (Internet Protocol Version 4) TCP/IPv4.

٧. اضغط أو انقر فوق الزر خصائص "Properties" أسفل القائمة

٨. اتبع الإعدادات على الصورة ادناه.

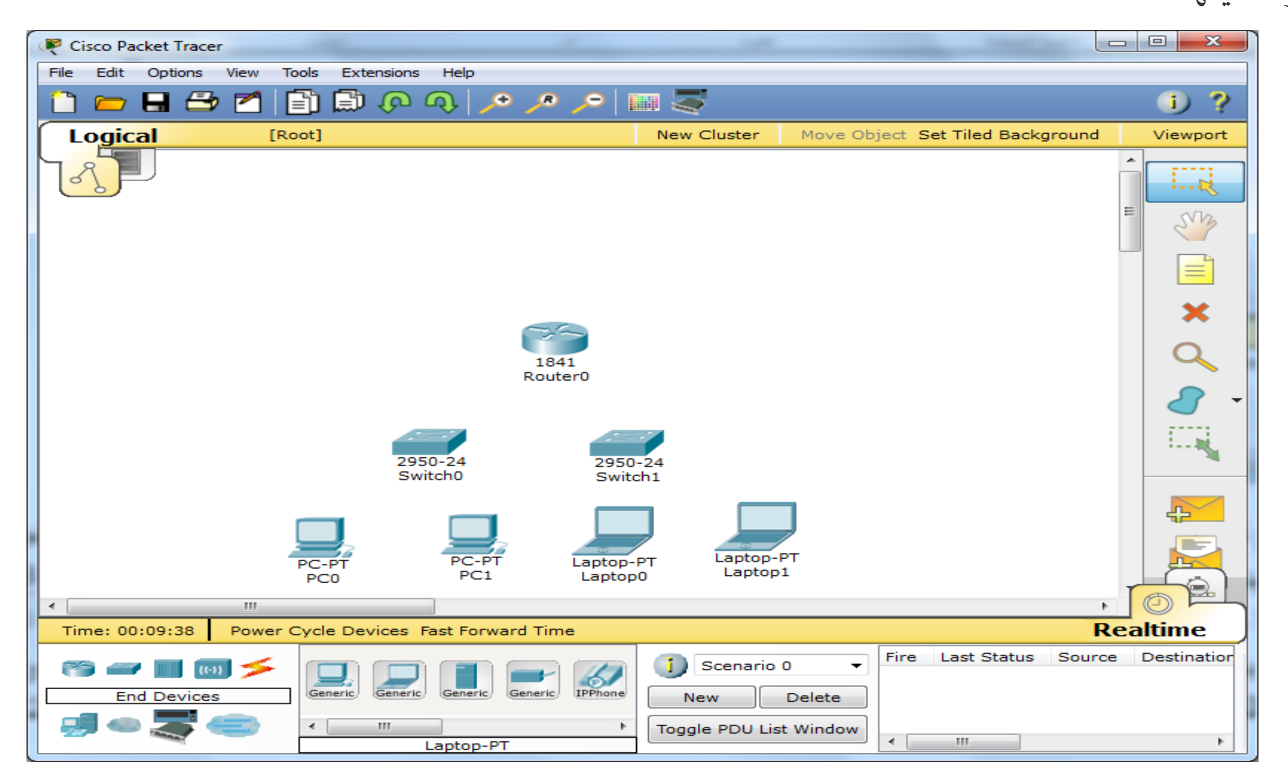


التطبيق الثاني؛ استخدام برنامج المحاكاة Packet Tracer:

أولًا: مقدمة عن برنامج Packet Tracer

يعتبر برنامج Packet Tracer من أهم البرامج لاستخدامه في محاكاه الشبكات وذلك لسهولة استخدامه لعمل بيئات لاختبار وتعليم الاتصال الشبكي. ويستخدم أيضا في تصميم وتطوير الشبكات حيث إنه برنامج سهل الاستخدام متعدد المهام ويحتوي على محاكاة لكافة أنواع المحولات (Switches) وأجهزة الموجهات (Routers).

بداية وبعد تنصيب البرنامج يتم فتح البرنامج من الاختصار الخاص به على سطح المكتب او من خلال قائمة Start. وكمو في أي برنامج تطبيقي تتكون الواجهة من عدة أجزاء ففي الأعلى تقع القوائم والأدوات المعروفة مثل قائمة ملف File وقائمة تحرير Edit وهكذا واما ما يهمنا هنا في دراستنا فهو الجزء الأسفل من النافذة الذي يحتوي على مؤقت لمدة عمل البرنامج ومجموعة ايقونات لأجهزة وأسلاك وأدوات الربط للشبكات ويمكن النقر على أي منها أو سحبها لإضافتها إلى وسط النافذة، وهو الجزء الأبيض المستخدم لبناء الشبكة وتصميمها.



كما بالصورة أعلاه تم إضافة بعض الأجهزة وذلك لترتيبها واستخدامها لبناء شبكة متكاملة

عملية ربط الأجهزة:

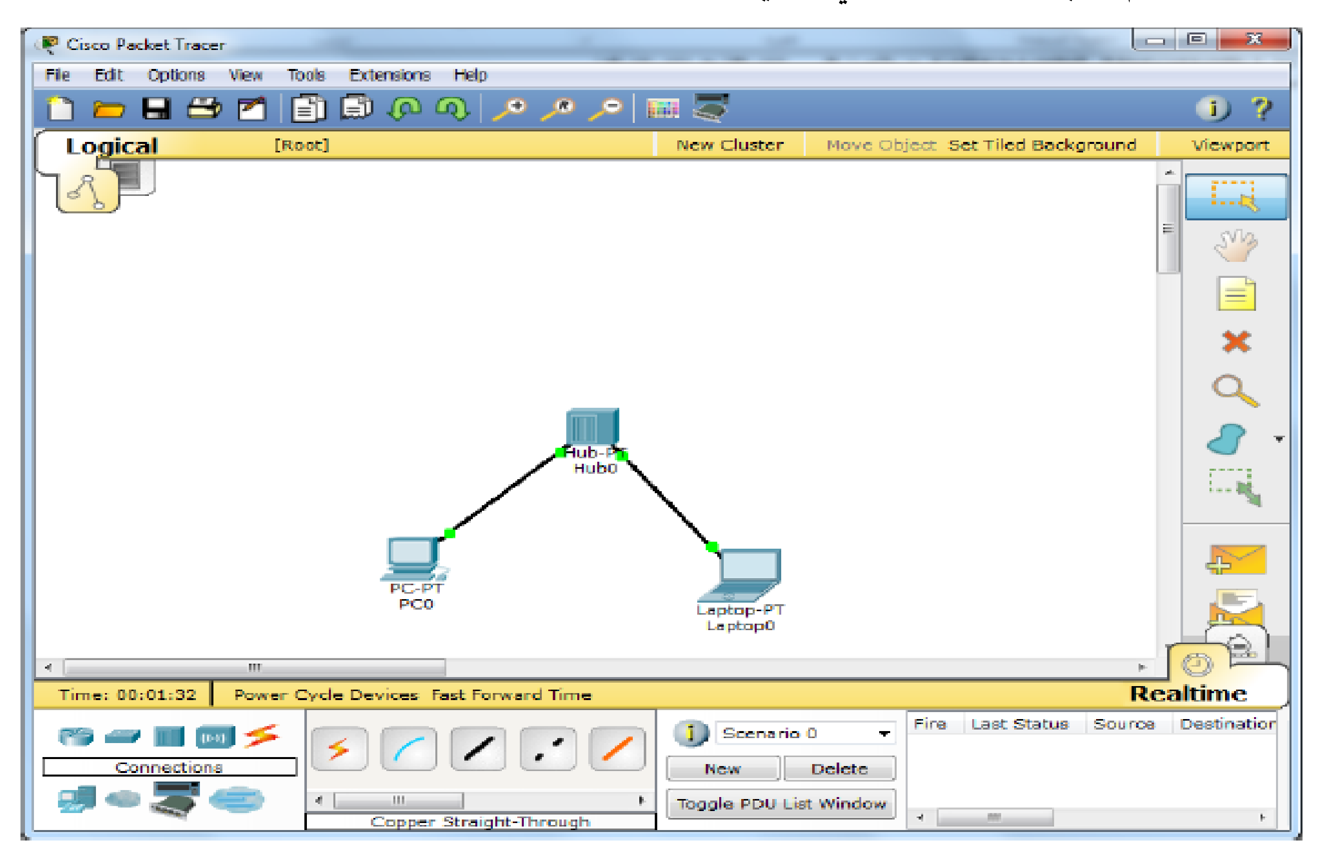
بخصوص ربط الأجهزة كما هو معلوم هناك العديد من أنواع الاسلاك التي تستخدم في عملية الربط الشبكي وللتعرف على طرق الربط ننظر في الجدول أدناه:

نوع الربط	صفاته	استخداماته
Straight Through	الربط المباشر وتكون كلا طرفي السلك متشابهين وبنفس الترتيب	يستخدم لربط الاجهزة المختلفة اي من حاسبة الى سويتش او من سويتش الى موجه او من حاسبة الى موزع (hub) وهكذا.
Cross Over	الربط الانتقالي ويتم قلب ترتيب الاسلاك بين الطرف الاول والثاني كالاتي: الاول==الثالث الثاني==السادس الثالث==الاول السادس==الثاني واما بقية الاسلاك الاربعة فتبقى على نفس ترتيبها في طرفي الكيبل	يستخدم لربط الاجهزة المتشابهة اي من حاسبة الى حاسبة او من موزع الى موزع ولكن هناك ملاحظة مهمة وهي ان الحاسبة والموجه يعتبران جهازين متشابهين (PC=Router) وكذلك الموزع (Hub) والسويتش (Switch) يعتبران متشابهين (switch=hub) فيتم ربطهما بهذا النوع
Roll Over	يتم عكس كل الاسلاك الثمانية في الطرف الاول عن الطرف الثاني وكالاتي: الاول=الثامن الثاني=السابع الثالث=السادس الرابع=الخامس الخامس=الرابع السادس=الثالث السابع=الثاني الثامن=الاول	يستخدم لربط الموجه (Router) الى الحاسوب عبر منفذ البرمجة (Console Port) والذي من خلاله يتم برمجة الموجه من نوع سيسكو فقط عن طريق الحاسوب.

الدرس الثالث: استخدام برنامج Packet Tracer (التطبيق الأول)

بعد أن تعرفنا في الدرس الأول علي واجهة البرنامج وكيفية إضافة العناصر إلى واجهة التصميم الخاص به؛ سنقوم الآن ببدء أول تطبيق عملي للبرنامج وذلك بإضافة عدد ٢ جهاز حاسوب) وإضافة الإعدادات الخاصة بالربط الشبكي لهذه الأجهزة وربطها باستخدام جهاز Switch وإجراء الاختبار الشبكي للتأكد من أن هذه الأجهزة متصلة شبكيا.

١. افتح البرنامج.
٢. نقوم بإضافة عدد ٢ جهاز اما باستخدام PC وأLaptop.
٣. نقوم بإضافة جهاز سويتش.
٤. نختار سلك الربط بالضغط علي علامة الصاعقة ونختار نوع التوصيل Strait through كما هو بالشكل التالي.
٥. نقوم بالربط من كل جهاز الي السويتش.

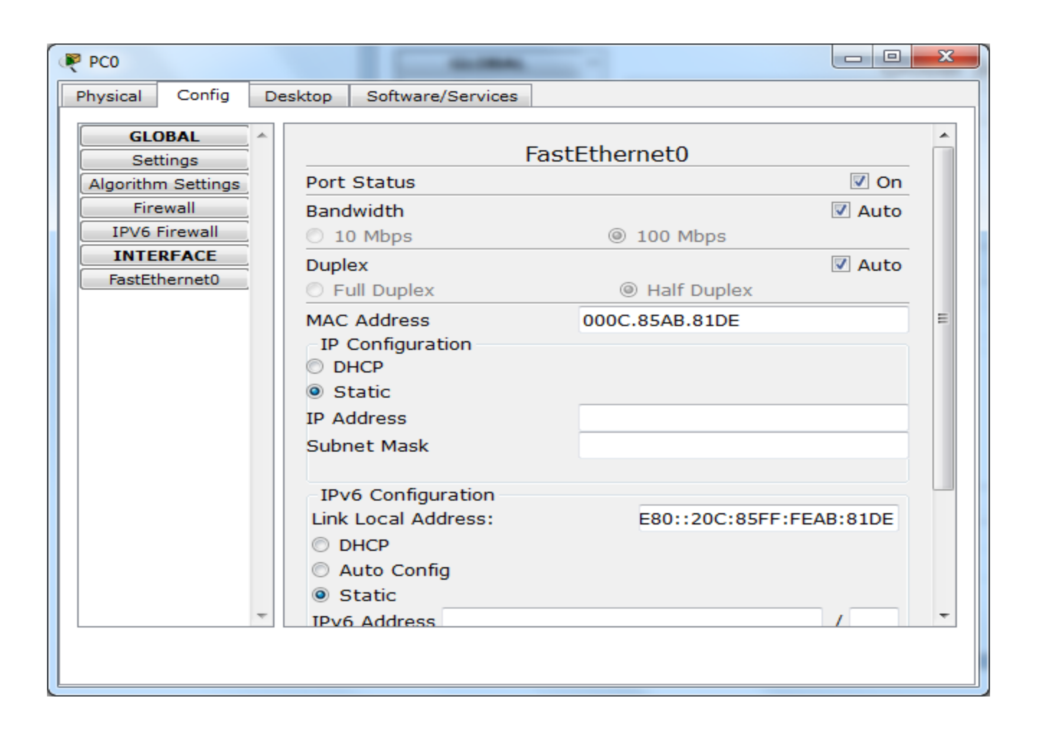


الآن نقوم بوضع الإعدادات، وإسناد العناوين المنطقية Ip address لكل حاسبة من الحاسبات المرتبطة بالشبكة، وهو نفس الأمر الذي يحصل في الواقع. فبعد ربط الأسلاك في الشبكة يجب إسناد IP address لكل جهاز مرتبط بالشبكة، ويشترط بالعناوين المسندة إلى الحاسبات ضمن الشبكة المحلية LAN أن تكون من نفس Class، وأدناه جدول مختصر يوضح الفئات العامة IP Classes المستخدمة في الشبكات بشكل تلقائي:

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

وتعرف هذه العناوين المحددة في الجدول بالعناوين الخاصة (Private IP Address) والتي يمكن استخدامها لربط الشبكات المحلية LAN Network، ولعل ذلك في التمرين الحالي نقوم بالنقر المزدوج Double Click على الجهاز الأول ومن تبويب Config نقوم بوضع الإعدادات كما يلي:

١. اضغط على Fasstethernet0 من الجزء الأيسر كما بالنافذة أدناه واختار Static.

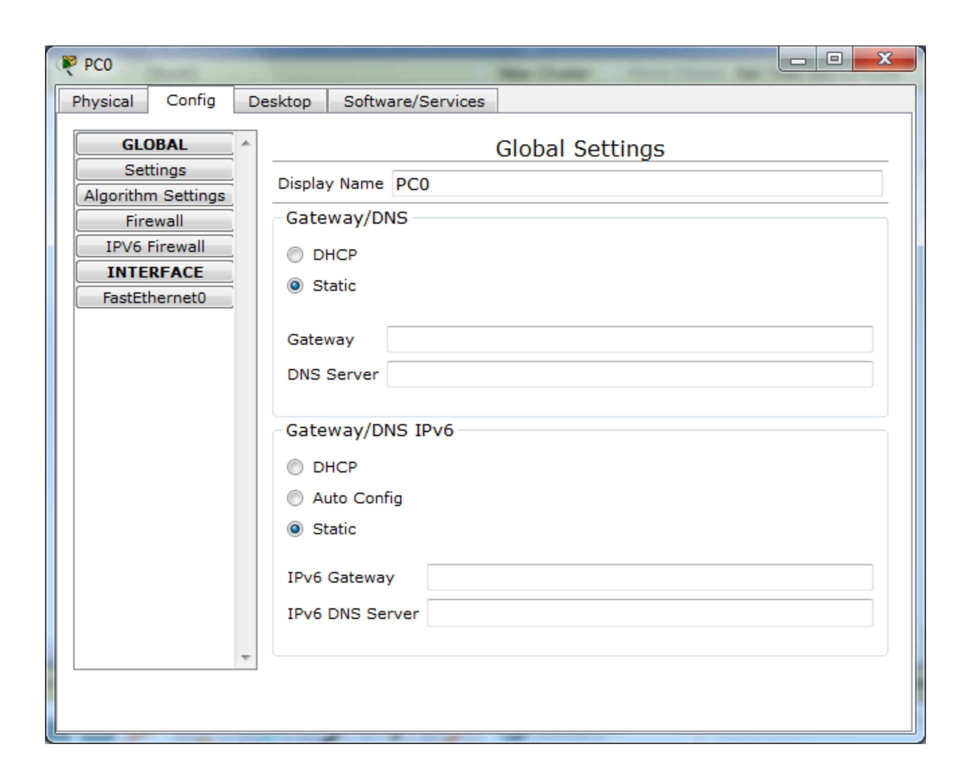


٢. قم بكتابة الإعدادات الخاصة بهذا الجهاز

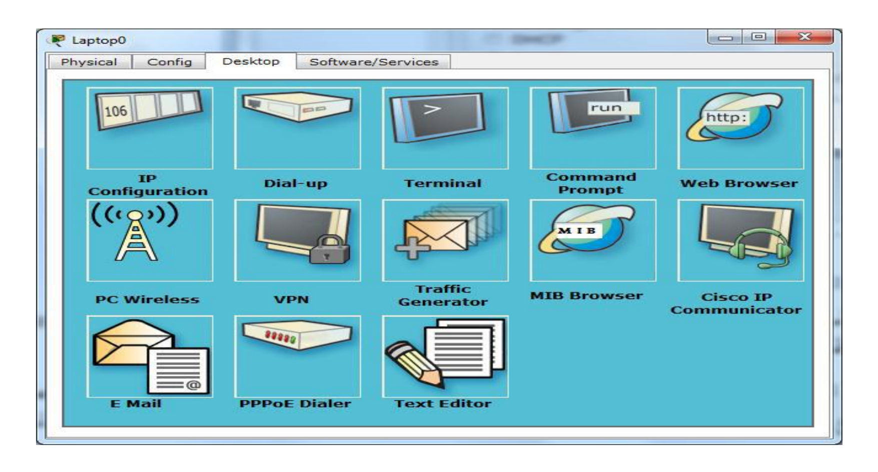
(a) Ip Address وليكن مثلا 192.168.1.5

(b) Subnet mask 255.255.255.0

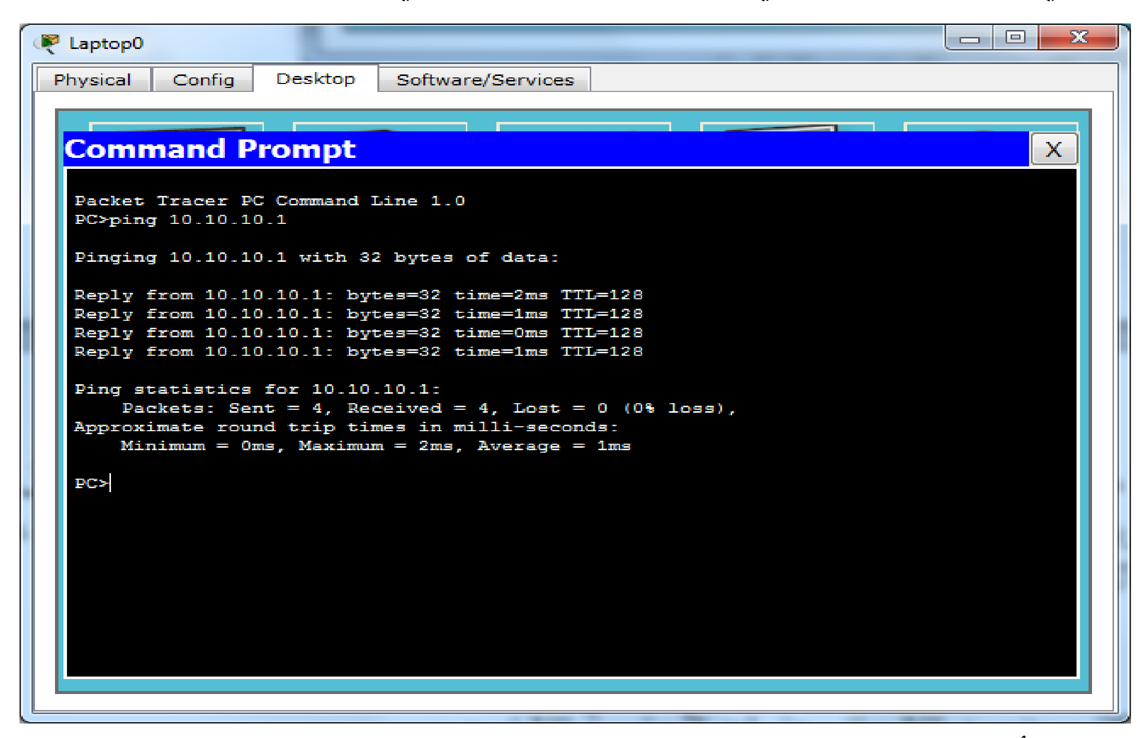
٣. قم بتكرار الخطوات السابقة على الجهاز الأخر كما بالصور.



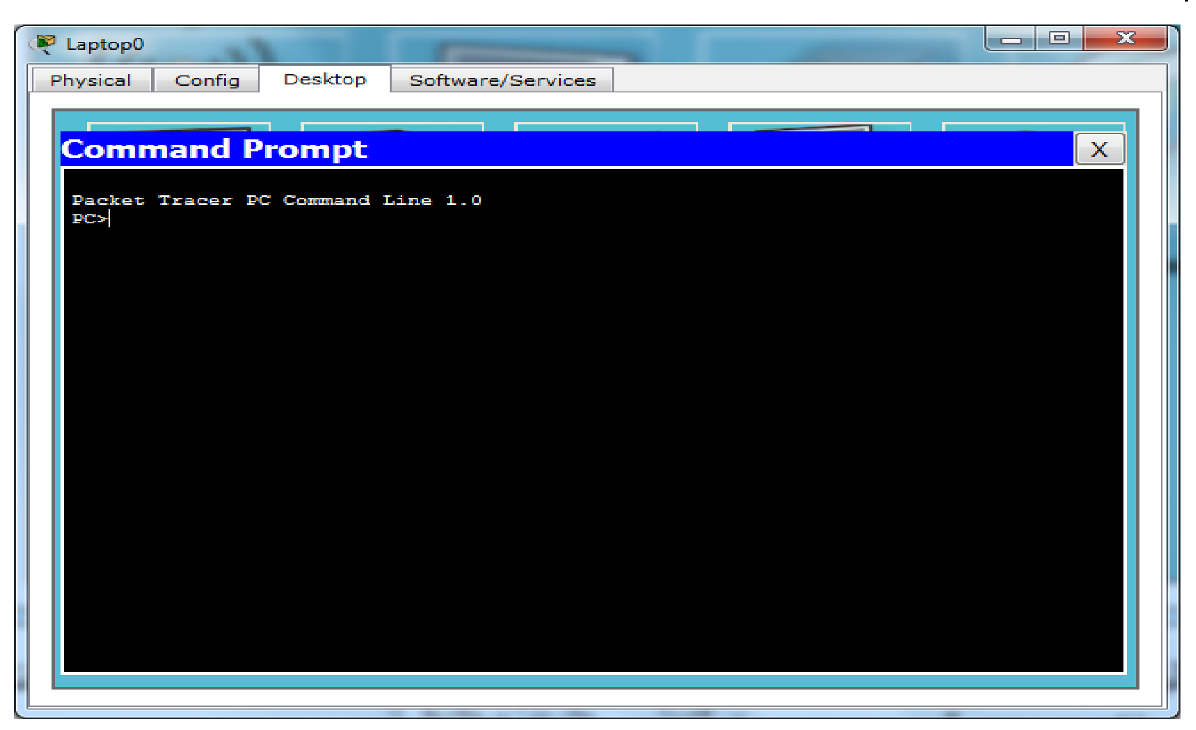
الآن وبعد إكمال الإجراءات أعلاه نقوم بالخطوة الأخيرة؛ وهي اختبار عمل الشبكة وهل يوجد اتصال شبكي بين الأجهزة أم لا، ولفعل ذلك نستعين بالأدوات المرفقة مع كل أيقونة حاسوب PC وذلك عن طريق الذهاب إلى تبويب Desktop واتباع الآتي:



نلاحظ ان هناك الكثير من البرامج الموجودة سنستخدم CMD وذلك لعمل اختبار للاتصال بعدها يمكن استخدام أدوات مدير الشبكة لاختبار الاتصال ومن أهم هذه الأدوات خو امر (PING) وهو من أهم الأدوات المستخدمة في اختبار الاتصال الشبكي Ping IP address كما في النافذة التالية:



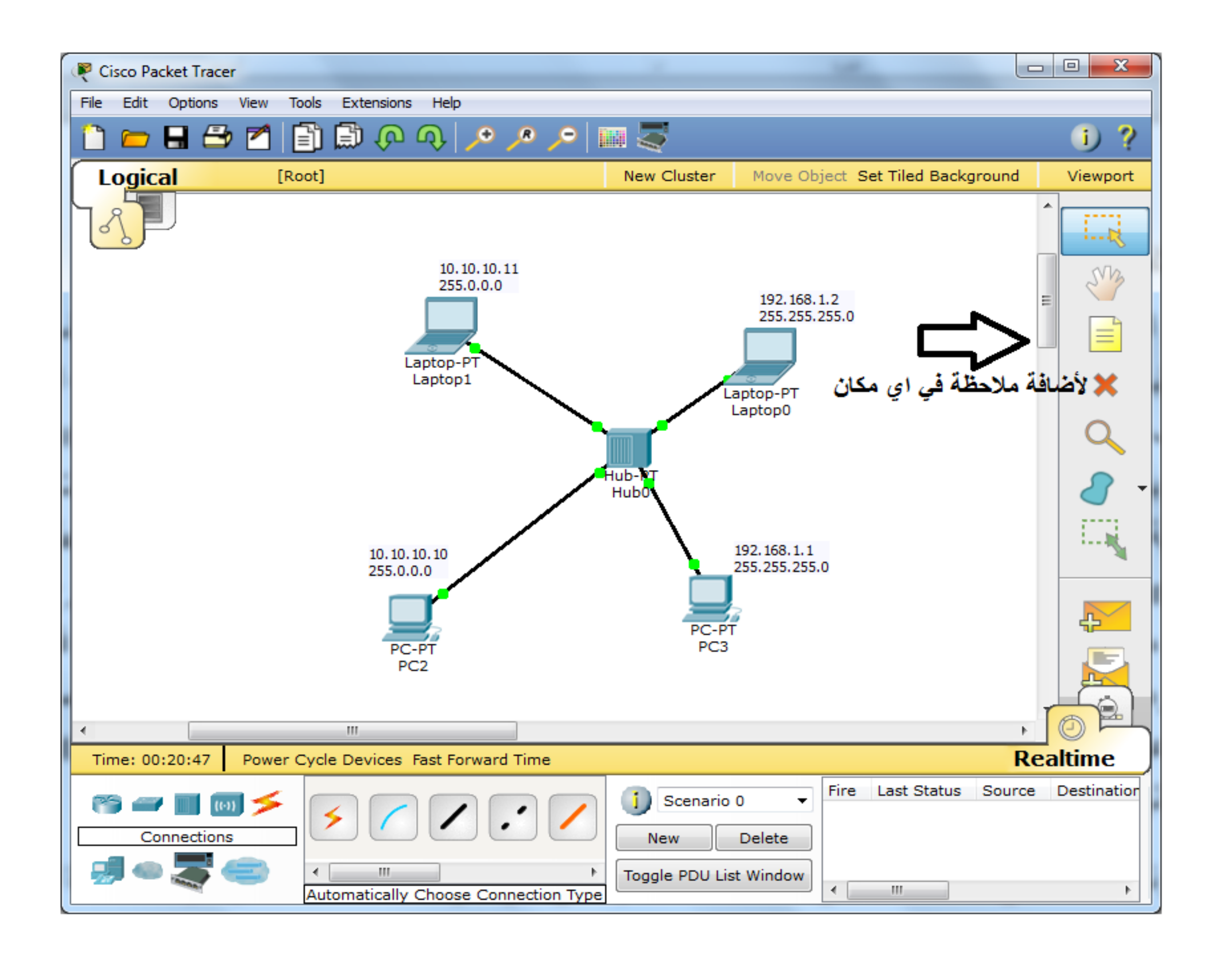
ونقوم بتركيز الأمر في الجهاز الآخر وكما نرى لدي الاختبار على وجود اتصال بين الجهازين نتيجة وجود reply.



التطبيق الثاني (اختبار مدي فهم برنامج Packet tracer)

في هذا التطبيق سيتم ربط أربعة أجهزة من نوع PC أو Laptop عن طريق استخدام جهاز محول Switch: قم بكتابة الخطوات بنفسك وتحقق من اتصال الأجهزة ببعضها بالاعتماد على البيانات الموجودة على الصورة ادناه.

ملاحظة مهمة لكتابة بيانات الأجهزة كما بالصورة أدناه نستخدم أداة الملاحظات أو التعليقات.



تطبيقات إضافية شرح بواسطة المدرب

1. استخدام برنامج VMware لشرح تثبيت ويندوز سيرفر ٢٠١٢ واعداد خادم DHCP وخادم DNS
2. باستخدام برنامج Packet tracer قم بربط عدد ٣ أجهزة ومجموعة Switch مع ربط جهاز خادم DHCP واجعل الأجهزة تأخذ اعدادات Ip باستخدام خدمة DHCP من هذا الخادم.